DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC REGULATION NO. 525-13

17 February 1999

Military Operations

AMC FORCE PROTECTION PROGRAM

Supplementation. Supplementation of this regulation is permitted with prior written approval by HQ AMC (AMCLG-OF), DSN 767-0672 or COM (703) 617-0674. When supplements are approved and issued, one copy will be furnished to HQ AMC (AMCLG-OF). Requests for exceptions to this regulation, with justification, will be sent through command channels to the AMC Force Protection Management Office (AMCLG-OF).

CHAPTER 1

INTRODUCTION

1-1. Overview. a. Force Protection (FP) is an integrated program developed to protect soldiers, civilian employees and contractors, family members, facilities, and equipment, in all locations and situations against the full spectrum of threats through the application of comprehensive programs and actions.

b. DA recognizes the probability of future attacks including terrorism, electronic data base destruction, etc., against U.S. defense assets in continental United States (CONUS) and outside CONUS (OCONUS). The intent of the Army Materiel Command (AMC) Force Protection Program (FPP) is to present command guidance to deter, defend, and react to possible threats or attacks directed against the AMC personnel and resources. This is accomplished by the planned integration of physical security, personal security, law enforcement operations, Information Assurance/Command & Control (IA/C2) protect operations, and operations security (OPSEC), all supported by the synchronization of training, operations, intelligence, policy, procedures, and resources.

c. This regulation defines the AMC FPP and implements National, Department of Defense (DOD), and Department of the Army (DA) antiterrorism (AT)/FP policies within AMC.

1-2. Applicability. a. This regulation applies to Headquarters (HQ) AMC; AMC major subordinate commands (MSC) and separate reporting activities (SRA) including subordinate facilities, installations, depots, plants, labs, operations, activities, sites, and ships.

b. This regulation applies to all AMC personnel - military and civilian, whether located on or off AMC installations. It applies at home station, during mobilization, deployment, overseas temporary duty (TDY) and during permanent change of station (PCS) moves. When contractors are on AMC properties pursuant to contract, they will observe AMC Force Protection guidance.

1-3. Commander's intent a. Antiterrorism/Force Protection is my most important priority. It is essential that each AMC commander, manager, and member of the Command, treat antiterrorism/force protection with the same high degree of significance and attention.

b. The protection of AMC people, facilities, and assets is an inherent command responsibility. I hold commanders accountable to create a secure and safe environment for their soldiers and civilians. I expect my commanders to remain personally involved in their force protection programs.

c. Each member of the command must support the AT/FP Program for it to succeed. The lives of our soldiers, civilians and their family members are too precious for us to place them at risk by doing anything less than our best to protect them.

1-4. References. Required and related publications are listed in appendix A.

1-5. Explanation of abbreviations and terms. Abbreviations and special terms used in this regulation are explained in the glossary.

CHAPTER 2

COMMAND FORCE PROTECTION POLICY

2-1. General. AMC commanders, directors, and supervisors will include FP measures in the planning and execution of all operations and activities. FP measures will be adequate and appropriate to reasonably safeguard soldiers, civilian employees, contractors, family members and critical assets. FP plans will clearly define the appropriate responsibilities and procedures for risk management, consequence response and decision-making.

2-2. Commanders and directors. a. Commanders and directors at all levels are responsible for Force Protection (FP) within their organizations, installations and facilities. AMC commanders must have functional plans to manage their FP programs, provide training, and issue guidance to their subordinates. FP policy matters that cannot be resolved at the local level will be brought to the attention of the next level in the chain of command.

b. Commanders will ensure that FP plans and procedures within AMC adhere to DOD and DA guidance and standards. Plans will be designed to deter incidents, and mitigate their effects to sustain the ability, as much as possible, to carry out assigned missions while providing a continuing level of protection for personnel, and critical equipment and facilities.

2-3. The individual. Individual responsibility is a key factor for an effective FP program and each individual within AMC must actively contribute to FP. Every member of AMC must develop and maintain an awareness of current threats, report suspected or actual threats, and take appropriate precautions and actions when confronted with an FP-related incident.

2-4. Coordination between installations and tenants. AMC organizations that maintain offices, facilities, or activities as tenants on host installations will ensure that FP standards and safeguards for AMC personnel and equipment, not achieved through organic resources, are otherwise accomplished through coordination with installation commanders. FP issues and services will be clearly addressed and identified in documents that define the relationship between host and tenant organizations (e.g., Terms of Reference, Memoranda of Understanding, Memoranda of Agreement). AMC Installations have the responsibility to ensure tenant organizations are included during FP planning.

2-5. Resources. Resources and assets must be prioritized. Force Protection resource requirements necessary to meet established standards will be identified, prioritized, and budgeted. Where local resources are insufficient to meet minimum standards, commands will forward prioritized and justified

requirements (**with appropriate impact statements**) to the next higher headquarters and initiate appropriate compensatory measures. Core element proponents (physical security, personnel security, law enforcement and information assurance/C2 protect) and installation commanders will ensure that measures necessary to meet established FP/security standards are adequately resourced or identified for funding. In addition, technology, where cost effective and appropriate, will be incorporated to the maximum extent possible to detect, delay, mitigate, and respond to acts of terrorism.

2-6. Risk management. Commanders and decision makers will employ risk management principles and processes as prescribed in DA Pamphlet 190-51 and FM 100-14, Risk Management, for requirements and development of FP plans. FP plans will include leaders at every level in identifying opportunities to integrate risk management into their organizations, tasks, and missions to effectively apply the process and control losses. Protecting the force through integration of safety into all aspects of planning and execution is critical to successful operations. Safety as a component of the protection element of combat power makes leaders responsible and accountable for protecting the force.

2-7. Training. a. Commanders will conduct and incorporate individual and unit level FP training into organization and activity Training Plans. All deploying individuals (soldiers, civilian employees, contractors, and family members traveling on official orders) will receive individual Level I AT/FP awareness training as mandated by AMC, AR 525-13, and applicable DOD directives prior to all travel and deployments outside the 50 United States, its territories and possessions.

b. Commanders will ensure procedures are in place to record and document Level I AT/FP training received by individuals.

2-8. THREATCON system. a. The intent of the Threat Condition (THREATCON) system is to implement appropriate protective measures to reduce the vulnerability of personnel and facilities. Establishing and implementing comprehensive THREATCON procedures is a primary factor in protecting personnel prior to an incident and providing a timely response after an incident.

b. AMC organizations will ensure compliance with all THREATCON procedures and standards as specified by regulation and DOD directives. Commanders will tailor THREATCON procedures to installation/geographic specific requirements. See paragraph 5-30d of this regulation for AMC specific reporting requirements. ***Appendix B (THREATCON System) to AR 525-13 contains required security measures for each THREATCON level***.

c. Commanders will report annually on their ability to implement THREATCON security requirements (reference paragraph 3-20).

CHAPTER 3

RESPONSIBILITIES

3-1. AMC Headquarters. Command and staff responsibilities for HQ AMC are outlined in AMC Circular 525-1 (to be replaced by an AMC Regulation). The Deputy Chief of Staff for Logistics and Operations (DCSOPS), AMCLG, HQ AMC, has overall responsibility for planning and coordinating the Force Protection Program within AMC. Operating under the DCSOPS, the AMC Force Protection Management Office (FPMO) will establish, implement and monitor FP policy within AMC. The FPMO coordinates with the FP core elements and other supporting staff sections to ensure a focused Force Protection Program is implemented throughout the command. AMC Headquarters will--

a. Maintain a Staff Assistance Visit (SAV) Program to ensure AMC FP programs and policies are properly implemented at all AMC organizational levels.

b. Publish guidance to subordinate commands for implementation of the Army FP standards (AR 525-13) and the AMC FP Program.

c. Establish a Command FP Committee and Working Group and appoint a Command FP Officer and Alternate/Assistant FP Officer.

d. Ensure that Sabotage and Espionage Directed Against the Army (SAEDA) training (AR 381-12) includes basic information on the nature of the terrorist threat, vulnerabilities of military personnel, civilian employees and their family members to terrorist acts, and individual self-protection.

e. Coordinate development of FP education and training programs, threat briefings, and public affairs command information programs to inform and increase antiterrorism and personal protection awareness among military and civilian personnel and their family members. Such materials will be disseminated on a routine basis at all AMC locations, with increased emphasis during periods when the THREATCON level exceeds NORMAL at CONUS locations or exceeds ALPHA PLUS at OCONUS locations.

f. Develop procedures to ensure that personnel traveling (on leave, temporary duty (TDY), permanent change of station (PCS), deployments and/or rotations) to countries that pose or potentially pose a physical danger, receive the appropriate AT/FP Level I training per AR 525-13 prior to initiation of travel.

g. Develop, coordinate and disseminate policy regarding organization, staffing, training and utilization of Special Reaction teams (SRT) on AMC installations.

h. Conduct FP compliance reviews of FP operations plans, operations orders, and/or standing operating procedures (SOP) developed by AMC MSCs, SRAs, and installations at least once every

2 years, or sooner, if required by major revision or installation/command realignment. Ensure that these plans, orders, or SOPs are exercised at installation level on an annual basis per AR 525-13.

i. Conduct an installation level comprehensive FP program review and FP assessment of each subordinate organization at least once every 2 years.

j. Coordinate requirements and funding for unique FP training.

k. Establish a system to monitor expenditure of FP funds from programming through budget execution with particular emphasis on (but not limited to): Management Decision Packages (MDEP) QLPR (Security Law Enforcement), RJC6 (Physical Security), VTER (Antiterrorism), and QSEC (Director of Security). In order to ensure adequate funding is maintained in these MDEPs from OMA, OPA-3, and RDTE appropriations, prioritization reviews will be conducted with cognizant AMC staff elements to ensure FP requirements are considered at Headquarters, Department of the Army (HQDA) and AMC Resource Action Committees (RAC).

l. Ensure that FP design measures have been considered and included, as appropriate, in the command's construction program per AR 415-15. Ensure that recommended protective measures are based on risk and threat analysis.

m. Coordinate the designation of high-risk personnel and the establishment of protective service missions and organizations within the command.

n. Establish written procedures for disseminating time sensitive threat information during duty and nonduty hours. Ensure that MSCs, SRAs, installations, and separate elements as deemed necessary by commanders, have developed and implemented supporting procedures.

o. Actively monitor the Force Protection programs of subordinate commands and SRAs.

p. Chapter 4 of this regulation describes the primary core elements of Force Protection and the AMC staffs that serve as proponents for each FP element. Core proponents are responsible for the management of their component programs and for the coordination of Force Protection actions with the AMC Force Protection Management Office.

3-2. Major subordinate commands (MSC) and separate reporting activities (SRA). MSCs and SRAs (excluding SRA tenants addressed in paragraph 3-4) will implement the AMC Force Protection Program within their organizations and geographic areas of responsibility. Commanders of MSCs and SRAs will--

a. Ensure compliance and implementation of all DA/AMC AT/FP standards, AMC FP requirements and procedures.

b. Establish and maintain a formal force protection program and issue implementing guidance to subordinate organizations and activities.

c. MSC commanders and separate activity (excluding SRA tenants addressed in paragraph 3-4) will establish a Force Protection Committee, a Force Protection Working Group, and appoint in writing a command force protection officer and alternate/assistant force protection officer.

d. Ensure that SAEDA training (AR 381-12) includes information on the nature of terrorist threat, and the vulnerabilities to military personnel, civilian employees and family members to terrorist acts, and identifies self-protection measures.

e. Develop AT training programs, threat briefings, and public affairs Command Information Programs to inform and increase antiterrorism and personal protection awareness among military and civilian personnel and their family members. Such materials will be disseminated on a routine basis at all locations with increased emphasis during periods when THREATCON levels exceed NORMAL at CONUS locations and exceed ALPHA for OCONUS locations.

f. Ensure that personnel traveling outside the 50 United States (on leave, TDY, PCS, or organization deployments) receive AT/FP Level I training prior to the initiation of travel.

g. Ensure an SRT capability exists per AR 190-58. Whenever practicable, SRT capability should be provided by a federal, state, or local law enforcement agency or by another Service, per written agreements between the installation and the supporting agency. These Memoranda of Agreement should be maintained with the Provost Marshal. Where practicable, commanders in OCONUS areas should request SRT support from host nation police agencies. Commanders should assess the capability of their own organizations and of supporting agencies to perform the SRT mission per AR 190-58. If SRT capabilities are insufficient or unsatisfactory, commanders will elevate the issue in writing to the next higher commander.

h. Review FP operations plans, operations orders, and or SOPs developed by subordinate organizations annually, or sooner if needed due to revised policy, or warranted by major changes in organizational or command structure.

i. Ensure that FP plans, orders, or SOPs are exercised at installation level on an annual basis and include all functional representatives (including civilian support agencies, when appropriate).

j. Program funds and identify personnel to attend specialized FP training. Ensure that all personnel with significant FP responsibilities in operations, intelligence, criminal investigations, facility engineers, public affairs officers, safety staff and Provost Marshal staff sections receive FP-related training.

k. Establish a system to monitor expenditure of FP funds from programming through budget execution.

l. Ensure that FP design measures have been considered and included, as appropriate, in the command's construction program per AR 415-15. Ensure that recommended protective measures are based on risk and threat analysis.

m. Recommend designation of high-risk personnel/position (HRP) to HQ AMC (AMCPE-S) per AR 190-58 and AR 525-13 and the establishment of full-time Protective Service organizations per 190-58, when required.

n. Include written procedures for disseminating time sensitive threat information during duty and nonduty hours in AMC FP Plans. Ensure subordinate organizations, installations, and separate elements as deemed necessary by commanders have developed supporting procedures.

o. Prior to 15 November each year, provide the Commander, AMC (AMCLG-OF), an assessment of Force Protection within his/her organization for the previous fiscal year. The assessment will include:

(1) A narrative discussion of the command's FP status.

(2) A copy of the updated MSC FP plan.

(3) Identification of all Force Protection upgrades completed during the preceding fiscal year (including subordinate elements).

(4) The amount of funds spent on Force Protection upgrades during the preceding fiscal year (including subordinate elements).

(5) Programmed FP upgrades for the next fiscal year (including subordinate elements).

(6) Ability/inability of command/organization to implement and sustain the various THREATCON security requirements (including subordinate elements). Detailed information is required for those measures that cannot be implemented. A generalized statement will suffice for THREATCON measures that can be effectively implemented.

(7) A prioritized list of unresourced FP projects, with justification and impact statement (including subordinate elements).

(8) A summary of lessons learned from the annual FP exercise (including subordinate elements).

p. Ensure implementation of Information Systems Security (ISS)/Information Assurance (IA) minimum-security requirements identified in AR 380-19 by all subordinate activities.

3-3. AMC installations. AMC Installation Commanders will--

a. Establish an installation Force Protection Committee and a Force Protection Working Group per this AMC regulation, and officially appoint in writing an installation force protection officer and alternate/assistant force protection officer. Within AMC, FP officers and alternate/assistant FP officers will be FP functional personnel, responsible for day-to-day program actions and functions. Individuals will not be appointed or certified as FP officers or alternate/assistant FP officers based solely on their duty position.

b. Designate in writing a prioritized list of mission essential vulnerability areas (MEVA). Indicate MEVA locations that are likely to be targeted by terrorists and other areas most vulnerable to terrorist attacks (e.g., housing areas, troop billets, schools, chapels, community centers, and other locations where large numbers of personnel reside or congregate).

c. Develop a comprehensive Force Protection operations plan or order which--

(1) Implements the Army AT/FP Standards (AR 525-13) and the AMC FP Program.

(2) Includes detailed installation level security procedures required at each THREATCON level (NORMAL through DELTA).

(3) Includes precautions appropriate to deter terrorist attacks against individuals and property.

(4) Is coordinated with the supporting Federal Bureau of Investigation (FBI) office, local supporting military intelligence (MI) organization, and appropriate state and local law enforcement agencies, or if OCONUS, with host nation security and law enforcement agencies.

(5) Includes emphasis on security of HRP and personnel whose official duties require presence outside the Army community.

(6) Describes procedures for responding to terrorist incidents occurring on the installation, facility, or activity.

d. Review installation and supporting Force Protection operations plans, and orders on an annual basis. Retain a written record of such reviews for 2 years following their completion.

Exercise installation level FP plans, orders, and SOPs on an annual basis. Medical response and mass casualty scenarios will be exercised annually. Retain exercise results and lessons learned for 2 years following completion of the exercise.

e. Prepare an installation/local security threat assessment that describes the current threat, to include criminal acts, foreign intelligence, paramilitary forces, saboteurs, protest groups, information system intruders/attackers, and disaffected persons. Assessments will be prepared at least annually (updated as required) and form the basis for identifying vulnerabilities that require correction. Various threats to morale, health, and welfare within the command should also be addressed.

f. Ensure that personnel with significant Force Protection responsibilities in operations, intelligence, public affairs, facility engineers, safety staff, and Provost Marshal staff sections have received appropriate FP-related training as specified in AR 525-13.

g. Ensure that Force Protection design measures have been considered, and, where appropriate, incorporated in the installation’s military construction design program and master plan.

h. Ensure that risk analyses for all new construction projects and renovations of Mission Essential Vulnerable Areas (MEVA) are performed per procedures outlined in DA PAM 190-51.

i. Establish and implement an installation THREATCON commensurate with the terrorist threat, existing vulnerabilities, and additional factors outlined in AR 525-13. Include detailed procedures for the implementation of threat measures and the dissemination of the current THREATCON level to tenant organizations.

j. Ensure that SAEDA training (AR 381-12) includes information on the nature of the terrorist threat, vulnerabilities of personnel and their families to terrorist acts, and self-protection measures that can be employed to deter or defeat such terrorist acts.

k. Develop and administer Force Protection education and training programs, threat briefings, and public affairs command information programs to continually inform and increase antiterrorism and personal protection awareness among military and civilian personnel and their family members.

l. Identify and coordinate for, or establish a special reaction capability to provide an appropriate response to threats identified in threat assessments, vulnerability assessments, etc. Where appropriate, organize, train, equip and exercise an SRT using existing resources or coordinate with a civilian or host nation law enforcement agency, or with another military

installation, to provide such capability. SRTs will be exercised on at least an annual basis to ensure response plans are realistic and valid. Commanders will assess the capability of their own organizations and of supporting agencies to perform the SRT mission per AR 190-58. If SRT capabilities are insufficient or unsatisfactory, commanders will elevate the issue in writing to the next higher commander.

m. Establish a system to monitor expenditure of Force Protection funds from programming through budget execution and ensure representation at Resource Integration Committee (RIC)/Resource Action Committee (RAC) meetings to defend programs.

n. Establish written procedures for dissemination of time-sensitive threat information during duty and nonduty hours. Ensure that subordinate commands or organizations, through company (or equivalent) level, have developed supporting procedures.

o. Develop procedures to ensure that all AMC personnel traveling outside the 50 United States (on leave, TDY, PCS, or unit deployments/rotations) receive AT/FP Level I training prior to initiation of travel. Established procedures will include a method for recording validation of individuals receiving training (reference paragraph 5-29 for training requirements).

p. Incorporate installation physical security initiatives into the Installation Master Plan. These initiatives should reduce installation/facility vulnerabilities in a manner that deters terrorist attack and inspires an appropriate level of confidence in the installation’s ability to protect personnel and assets.

q. Consider tenant organizations FP requirements when establishing and implementing the installation’s Force Protection Program and define these requirements in written agreements (e.g., Terms of Reference, Memoranda of Understanding, Memoranda of Agreement).

r. Initiate required Force Protection reports (Terrorist Threat Reports (TTR), Terrorist Incident Reports (TIR), and THREATCONs) for the installation and provide timely copies to appropriate tenants.

s. Ensure installation operating procedures clearly identify staff element responsibility for Force Protection requirements.

t. Ensure the implementation of adequate ISS/IA countermeasures for protection of AMC information.

u. Designate a provost marshal (PM)/security officer who will serve as the focal point to receive and disseminate time-sensitive threat information regardless of source or type. The Force Protection Management Office (FPMO) will be kept informed of all imminent threat information.

v. Situations where DOD/DA/AMC FP standards cannot be met will be reported to HQ AMC, FPMO, (AMCLG-OF).

w. The installation safety manager will report and submit required accident reports per AR 385-40.

3-4. AMC tenant organizations and stand-alone activities. AMC elements operating as a tenant organization or as a stand-alone activity will coordinate with the host installation/command or geographic commander to ensure Force Protection measures are in place. AMC elements will comply with the requirements of DOD/DA/AMC FP directives and standards and those requirements imposed by the host organization. Situations where DOD/DA/AMC FP standards cannot be met will be reported to HQ AMC, FPMO. Commanders of AMC organizations that are tenants of major Army commands (MACOM), MSCs, or other DOD Services will--

a. Establish written agreements (e.g., Terms of Reference, Memoranda of Understanding, Memoranda of Agreement) with the host installation (or geographic support commander as applicable) to clearly establish specific Force Protection responsibilities. FP agreement documents will address the following items, as appropriate:

(1) Force Protection support responsibilities.

(2) Force Protection committee and working group membership.

(3) Procedures for distribution of threat information.

(4) Urgent threat warning and alarm systems.

(5) Resource management responsibilities.

(6) Level I training/travel briefing program responsibilities.

(7) Participation/coordination in FP exercises.

b. Officially appoint a force protection officer and alternate/assistant force protection officer in writing, and advise the host installation force protection officer and MSC of these appointments. The tenant force protection officer/or alternate will serve on the installation FP Committee and/or FP Working Group, if appropriate. In any case, the AMC tenant FP officer/or alternate will maintain regular contact with the installation FP Officer to ensure an effective exchange of FP-related information and that AMC FP requirements are addressed. Those organizations without sufficient personnel to warrant appointment of a FP officer and alternate, will ensure that a FP point of contact (POC) is identified to the host installation.

c. Ensure the organization is covered by the host

installation's Force Protection Plan. If the installation does not have a Force Protection Plan, or the plan does not include FP for the tenant, the AMC tenant force protection officer will develop a Force Protection Plan for the organization and report the FP status and limitations to their parent command.

d. Develop procedures to ensure that installation specific threat information is received and distributed, as appropriate.

e. Identify Force Protection requirements for inclusion in host installation resource planning and programming.

f. Ensure personnel receive required Force Protection training and briefings through the installation, higher headquarters, or other sources as appropriate and/or available.

g. Implement appropriate security measures in response to THREATCONs established by the host installation and assist in implementing security measures, as required.

h. Participate in host installation Force Protection exercises, as appropriate.

CHAPTER 4

FORCE PROTECTION CORE ELEMENTS AND SUPPORTING STAFF COMPONENTS

4-1. General. FP pursues a systems approach that integrates existing security programs and procedures. The primary FP core elements are; physical security, law enforcement, personal security, Information Assurance and Operations Security (OPSEC). These elements are supported by additional staff components, as required. FP plans and operations should include input from personnel, resource management, intelligence operations, engineering, medical, public affairs, legal, safety, and chaplain services staff elements. The AMC FP Program integrates and synchronizes ongoing activities within these core elements and staff components (including proper use of OPSEC measures) to protect AMC assets from various threats.

4-2. Law enforcement. Army law enforcement activities support FP by deterrence of terrorist/criminal activity through the application of active law enforcement patrolling, crime prevention measures, liaison with local, state, and federal law enforcement activities, criminal investigations, and criminal intelligence collection. Law enforcement is a critical element of both emergency response procedures and consequence management.

4-3. Physical security. Physical security measures are designed to protect persons and property by deterring, detecting, and defending against physical intrusions into specific areas. Typical physical security measures include the use of physical barriers, electronic intrusion detection systems, access control procedures, routine inventories, and electronic surveillance. (AR 190-13)

4-4. Personal security. Personal security consists of those policies and measures designed to protect individuals and groups from attacks upon their persons. The program includes the protection of key figures as well as other individuals and spans the spectrum of simple, individually implemented self-protection and defensive measures, to more elaborate and direct individual protective service operations. (AR 190-58 and CID Regulation 195-1)

4-5. Information assurance/C2 protect. Information operations activities, collectively known as Information Assurance (IA), are essential to the protection of Army information infrastructures. IA functions encompass those continuous operations within the military information environment that enable, enhance and protect the friendly force’s ability to collect, process, and act on information to achieve an advantage across the full spectrum of military operations. IA operations include interacting with the global information environment and exploiting or denying an adversary’s information and decision capabilities.

In the context of AMC Force Protection, information operations consist mainly of Command and Control (C2) Protect, specifically Information Systems Security (ISS). (AR 380-19)

4-6. Operations Security (OPSEC). The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary. In the case of FP, it may be desirable to release certain information that reveals certain strengths and/or procedures, i.e., unannounced vehicle inspections, and change in guard post manning from time to time. These may serve as a deterrent. The intent being the harder the target, the less likelihood of attack. OPSEC is not intended to be a replacement for traditional security programs developed to protect classified information. OPSEC must be incorporated throughout the entire AT/FP program, as well as in each supporting security program. Although the Military Intelligence Office provides threat assessments, and can assist in the identification of OPSEC vulnerabilities, each AMC individual is charged with the responsibility to report vulnerabilities to the organizations' operations section. Army and AMC OPSEC policies are contained in AR 530-1 and AMC Supplement 1 to AR 530-1.

4-7. Support components to force protection. An effective FP program must be fully supported and integrated into all staff functions and coordinated by a Force Protection Management Office. Although the bulk of the FP program is the responsibility of the primary proponent core element, all staff elements have a FP responsibility. Additional staff support components include--

a. *Intelligence*. Military Intelligence (MI) supports AMC's FPP by collecting, analyzing, producing, reporting, and disseminating intelligence on a wide spectrum of foreign threats to AMC. By identifying and assessing international threats and threat levels, intelligence provides early threat warning. In CONUS, MI provides the foreign aspects of local threats, while law enforcement collects, analyzes, and disseminates domestic criminal and terrorist threat information. The integration of foreign and domestic-related intelligence, and threat data, enables commanders to designate an appropriate THREATCON level. In order for AMC FP elements to effectively carry out their designated responsibilities, the integration and use of intelligence information and assets is critical.

b. *Resource/funding*. An effective resource management program is essential to ensure adequate resourcing of AMC FP requirements. Resource management supports the AMC FPP through the identification of funds for validated and prioritized FP requirements submitted by operational planners and installation program managers.

c. *Engineering*. Engineering support to AMC FP provides effective, unobtrusive, and economical protective designs to ensure the incorporation of physical security measures to

safeguard AMC personnel and assets. The engineering support role applies to new construction, retrofit of present facilities, and those facilities erected as part of a contingency mission.

d. *Public Affairs*. Public Affairs meets a primary challenge of Force Protection by ensuring an accurate, timely and rapid flow of information from the command to internal and external audiences. Such communications help reduce force vulnerability, support FP efforts and project a strong image to potential terrorists and the American people.

e. *Legal*. AMC legal offices provide legal support to AMC commanders and staffs on all aspects of FP planning and operations. The legal office will ensure that all FP planning and operations conform to the requirements of applicable laws, directives, regulations, and other authoritative policy documents.

f. *Chemical/biological*. The Soldier Biological and Chemical Command (SBCCOM) provides guidance to the AMC FP program for the protection of AMC personnel and assets against chemical and biological (CB) attacks, and technical assistance in response to a CB-related attack.

g. *Medical Services*. Medical support to the AMC FP program provides an immediate medical response to treat, and prevent casualties resulting from the use of weapons of mass destruction, or other attack means directed against AMC personnel and assets. This is achieved through a well-planned, coordinated, flexible, and resourced Response and Consequence Management Plan.

h. *Safety*. Safety support provides information to AMC commanders and staffs for the protection of AMC personnel and assets through identification, evaluation, and control of hazards. Integration of safety in FP plans, using the five-step risk management process, is a principal element in decision making.

CHAPTER 5

FORCE PROTECTION REQUIREMENTS AND PROCEDURES

5-1. General. All AMC organizations are required to comply with the FP guidelines, procedures, standards, and requirements as specified in AR 525-13 and the primary DOD FP policy documents. The DOD FP standards, as specified in DODI O-2000.16, have been incorporated into AR 525-13. This AMC FP regulation (AMC-R 525-13), used in conjunction with AR 525-13, provides additional information, which enhances, modifies, or restates the Army standards as they apply to AMC requirements.

5-2. Force protection plan. a. Force Protection is an integrated operations program developed to protect soldiers, civilian employees and family members, facilities and equipment, in all locations and situations. This is accomplished through the integration of C2 protect operations, personal security, physical security, law enforcement operations, training and OPSEC, all supported by the synchronization of mission operations, intelligence, policy and resources. The integration of staff elements in a FP plan is an essential factor in creating an effective FP program. All agencies involved in the program execution, to include non-DOD agencies at the local, state, and federal level, must be fully integrated into the program's development, coordination, and maintenance.

b. The time to begin detailed planning for responding to a FP-related threat or terrorist attack is before a threat develops or an attack occurs. Commanders at all levels will ensure Force Protection plans, orders, or other implementing guidance is realistic and comprehensive. These documents will prescribe both preemptive and defensive measures designed to reduce command terrorist threat vulnerabilities prior to a terrorist attack, and the detailed procedures for responding to an attack after it occurs. Resources and assets must be prioritized and the required level of protection, during various periods of time, must be clearly specified.

c. AMC commanders and directors of major subordinate commands (MSC), separate reporting activities (SRA), installations and deploying organizations will prepare a Force Protection Plan. FP plans will be updated/reviewed--

(1) Annually by the MSC, SRAs and installation/ organization.

(2) At least once every 2 years by the MACOM (reviewed).

(3) As required due to command or installation realignment, or major changes to installation vulnerabilities or threat.

d. At a minimum, the FP plan will cover, or include the following areas (those FP requirements provided by a host installation or other activity will be clearly identified):

(1) Implementation guidance for AR 525-13 and this AMC regulation; and, a description of the organizations AT/FP program.

(2) An assessment of the actual terrorist threat (or absence of threat).

(3) Clearly defined and localized protective and preventive measures to be initiated during periods of higher THREATCON. Forces or units required to implement FP measures will be specified, where appropriate. Outside agencies, if used, will be clearly identified.

(4) Appropriate actions for reporting terrorist incidents and threat information, and incident response.

(5) Procedures to request support from and/or notify the FBI, state and local law enforcement agencies in the event of a terrorist incident. The plan will also contain instructions on providing legally authorized support to the FBI, state or local law enforcement agencies, when requested in response to a terrorist attack in the civil communities.

(6) Organization, training, equipment, certification and operational procedures for the Special Response Team (SRT).

(7) Exercise procedures and identified scheduling procedure for testing the FP plan.

(8) Procedures to respond to natural and manmade emergencies.

e. All Force Protection staff efforts will be coordinated by the operations officer (or his equivalent), working closely with the Provost Marshal, intelligence officer, information management officer, resource management officer and other staff elements, as appropriate. In those headquarters organized without a separate and distinct operations staff element, the commander will formally assign responsibility for Force Protection to the staff principal whose functions most closely align with the operations function.

f. The Force Protection officer will ensure that as a minimum, in addition to the core staff elements, the intelligence, engineer, logistics, medical, Staff Judge Advocate (SJA), resource management, safety staff, and public affairs staff representatives are involved in all Force Protection planning considerations.

g. FP policy issues that cannot be resolved at the local level will be brought to the attention of the next higher AMC headquarters for resolution.

h. All operations plans and orders will contain an assessment of the actual threat (or absence of threat) and will prescribe appropriate actions for reporting terrorist threat and incident information (this requirement can be met by referencing an SOP or other document that is readily available to all organizations responsible for executing the plan or order).

i. Unit movement directives will contain instructions directing a predeployment orientation concerning the threat, including terrorism.

j. All organizations not otherwise required to develop Force Protection plans or orders, or address Force Protection-related concerns in other operations plans or orders, will incorporate Force Protection into existing documents (such as SOPs) which prescribe security procedures for the organization. At a minimum, Force Protection guidance incorporated into other policy documents will address specific, detailed procedures for implementing THREATCON measures described in AR 525-13.

5-3. Force protection officer. a. All AMC MSCs, SRAs, installations, and tenant activities will officially appoint, in writing, a force protection officer and an alternate/assistant force protection officer. Considering the importance of his/her duties and to ensure optimum effectiveness, the force protection officer should fall under the cognizance of the operations section or its operational equivalent. The force protection officer will--

(1) Represent the appointing command/organization/ activity for all FP-related issues.

(2) Be knowledgeable of DOD/DA/AMC FP policies and standards.

(3) Implement, comply with, and manage the FP program at their appointed level.

(4) Establish and chair the FP Working Group (if required at the appointed level).

(5) Keep the chain of command informed of FP status and present unresolved FP issues to the chain of command for assistance, action and resolution of the issue.

(6) Ensure the alternate/assistant force protection officer is kept informed of major FP issues.

b. The alternate/assistant force protection officer will--

(1) Be knowledgeable of DOD/DA/AMC FP policies and standards.

(2) Serve as the force protection officer when the primary FP officer is unavailable to perform the assigned duties.

(3) Assist the FP officer in the development, implementation and execution of FP programs.

5-4. Force protection committee. All AMC MSCs, SRAs, and installations will establish Force Protection Committees that meet, as a minimum, quarterly. Notes from these meetings will then be sent to AMC HQ (AMCLG-OF).

5-5. Force protection working group. All MSCs, SRAs, and installations will establish a FP Working Group that meets (at a minimum) monthly to discuss FP issues, the current terrorist threat, and evaluate FP security measures. FP Working Groups will provide FP options and policy changes as recommendations to the FP Committee for incorporation into the organization's FP program.

5-6. New commanders force protection checklist. All MSCs and SRAs will prepare a New Commander’s Force Protection Checklist that details the inherent obligations of commanders, their assigned area of responsibility, and identifies questions for commanders to consider. All incoming commanders will be provided the checklist prior to assumption of command per appendix W, DOD 2000.12H.

5-7. Crisis management plan and checklist. A Force Protection Crisis Management Plan, including a Force Protection Crisis Management Plan checklist (per appendix X, DOD 2000.12H), will be prepared at the installation level on how the commander will conduct combating terrorism operations. The FP Crisis Management Plan will be part of the installation FP Plan.

5-8. MACOM force protection periodic program reviews and vulnerability assessments. a. HQ AMC (AMCLG-OF) has proponency over the command inspection program to ensure compliance with DOD Army and AMC regulations and directives pertaining to Force Protection.

b. HQ AMC will form a Staff Assistance Visit (SAV) and Inspection Teams under the direction of the Deputy Chief of Staff for Logistics and Operations to conduct the program reviews and assessments. The team will consist of HQ AMC staff membership as required to conduct an effective compliance oriented review process.

c. HQ AMC (AMCLG-OF) will conduct periodic program reviews to subordinate commands to review FP programs and to perform FP vulnerability assessments of subordinate installations and organizations.

d. Advance parties for OCONUS deploying elements will include individuals with FP experience to evaluate current/potential FP

concerns. A report on Force Protection status will be provided to the deploying commander in time to allow for guidance and FP planning considerations.

5-9. THREATCON system. Per AR 525-13, Terrorist Threat Conditions (THREATCON) describe progressive levels of security measures for implementation in response to terrorist threats to U.S. Army personnel and facilities. Commanders at installation level and lower will develop **specific** instructions to implement measures identified in AR 525-13, Appendix B, for the five established THREATCON levels. The five levels are--

a. THREATCON Normal: Applies when there is no discernible threat of possible terrorist activity.

b. THREATCON Alpha: Applies when there is a general threat of possible terrorist activity.

c. THREATCON Bravo: Applies when an increased or more predictable threat of terrorist activity exists.

d. THREATCON Charlie: Applies when an incident occurs or intelligence indicates that some form of terrorist action is imminent.

e. THREATCON Delta: Applies in the immediate area where a terrorist attack has occurred or when intelligence indicates that terrorist attack is likely.

5-10. Operations security. a. OPSEC has a direct impact on the vulnerability of AMC personnel and assets. Readily available open source information can aid adversaries in targeting AMC assets and should be considered during FP planning and vulnerability assessments.

b. In addition to traditional OPSEC concerns, information posted to unclassified AMC web sites will be reviewed by the responsible staff office for possible OPSEC vulnerabilities. The OPSEC review should also include any AMC contractor or installation operated web sites. During increased THREATCON periods, curtailed or restricted access to AMC web sites should be considered as a possible security measure. The supporting MI office can assist in determining potential OPSEC vulnerabilities related to web sites.

c. Per AR 530-1, all plans must include an OPSEC annex. The OPSEC annex will address vulnerabilities, information to be protected, assessment of risks and the application of appropriate countermeasures. Using risk management procedures, each commander must establish the level of risk he will accept to complete the mission.

5-11. Information assurrance/C2 protect. a. C2 Protect operations safeguard AMC automated information systems (AIS) and the data thereon from unauthorized access, misuse or destruction through an effective employment of countermeasures and operation policy guidelines. Aggressive C2 operations will ensure system availability, data confidentiality (from unauthorized disclosure), data integrity (from unauthorized modification), and authentication (of authorized users) of AMC's data and systems. This protection is limited to those AIS that AMC assets operate or control however, AMC must ensure that adequate measures have been taken by Defense Information Systems Agency (DISA) and the Defense Megacenters (DMC) to verify that an adequate Continuity of Operations/Disaster Recovery Plan (COOP/DRP) exists.

b. AIS security is achieved through a layered approach. These layers consist of procedural security, physical security, software/hardware security, training and education, reporting procedures, and inspection/oversight. The application of specific layers of security is dependent upon the data and equipment value in support of the organization's mission.

c. Human threats to AMC's AIS and the data residing thereon come from "outsiders" and "insiders." Outsiders include hostile intelligence services, terrorist organizations, criminal elements, and hackers. Insiders include disgruntled and psychotic employees and untrained or careless employees. Environmental threats to AMC AIS must also be considered. Using a layered security concept of protective countermeasures, the following identifiable threats can be eliminated or minimized:

(1) Foreign Government agents (Outsider threat): Their goal is to access sensitive information, unclassified or classified, that will give their country a military, technological, psychological or economic advantage over the United States. Preferred means of attack is to co-opt an employee; other methods such as wiretaps, electronic eavesdropping, signals intercept, and hardware or software modification or tampering may also be used. The affected protection categories are: availability, confidentiality, integrity, and authentication.

(a) Countermeasures (include but are not limited to):

1 Ensure all known system vulnerabilities have been identified and/or eliminated.

2 Review audit trail information. Audit trails will provide sufficient detail to reconstruct events in determining cause and magnitude of damage.

3 Implement network protection (filtering) to protect and control Internet Protocol (IP) addresses.

4 Review access control procedures; ensure user-id's are authentic and passwords are generated, protected, and changed as stated in AIS security SOP and encrypted during transmission.

5 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

6 Notify all data owners of possible corruption and/or compromise of their data.

7 Invoke contingency plan with essential backup software to restore operations.

8 Notify appropriate agencies, i.e., the Land Information Warfare Activity (LIWA)/Army Computer Emergency Response Team (ACERT): **Commercial Phones** 1-888-203-6332 (STU-III), (703) 706-1113/1922 (STU-IIIs); **World Wide DSN** (312) 235-1113/1922 (STU-IIIs); **FAX** (703) 806-1152 (DSN 656-1152); **Secure FAX** (703) 806-1004 (DSN 656-1004); **NIPRNET** acert@acert.belvoir .army.mil; **SIPRNET** acert@inscom.army.smil.mil; **Tools E-mail** tools@acert.belvoir.army.mil; **Webmaster E-mail** webmaster@acert .belvoir.army.mil; **GENSER Address** RUDHAER// ACERT FT BELVOIR VA; **PGP Key** ACERTpubkey.txt (Updated 15 Dec 98) **Mailing Address** LIWA/ACERT, ATTN: Director, Suite B211, 8825 Beulah Street, Fort Belvoir, VA 22060-5246.

(b) Notification: Immediate supervisor, Information Systems Security Manager/Officer, Intelligence and Security Directorate, Provost Marshal (Criminal Investigation Command (CID), LIWA, FP Officer and local Military Intelligence element.

(2) Hackers (Outsider threat). "True" hackers are motivated by the challenge of breaking into a system to browse the system to determine its capabilities and vulnerabilities and to look for resources or information to use to break into other systems. "Malicious" hackers are also motivated by the challenge, but also to degrade or destroy all or parts of the system. "Info" hackers enter a system looking for information or data that can be exploited. The affected protection categories are: availability, confidentiality, integrity, and authentication.

(a) Countermeasures:

1 Ensure all known system vulnerabilities have been identified and/or eliminated.

2 Review audit trail information to determine magnitude of damage.

3 Implement network protection (filtering) to protect and control Internet Protocol (IP) addresses.

4 Review access control procedures; ensure user-id's are authentic and passwords are generated, protected, and changed as stated in AIS security SOP and encrypted during transmission.

5 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

6 Notify all data owners of possible compromise and/or corruption of their data.

7 Invoke contingency plan with essential backup software to restore operations.

8 Notify the ACERT, Comm (703) 706-1113.

(b) Notification: Immediate supervisor, Information Systems Security Manager/Officer, Intelligence and Security Directorate, Provost Marshal (CID), FP Officer, LIWA, and local MI element if damage to sensitive, classified AIS and/or foreign involvement is suspected.

(3) Terrorists (Outsider threat). Terrorists are usually motivated by a deeply held sense of grievance over some perceived form of injustice. Their objective is to draw attention to their cause through use of tactics that invoke fear in a target. Primary purpose for targeting AMC resources would be to obtain information and/or resources in support of future activities and attacks and to destroy capability. The affected protection categories are: confidentiality and integrity.

(a) Countermeasures:

1 Review audit trail information to determine magnitude of damage.

2 Implement network protection (filtering) to protect and control Internet Protocol (IP) addresses.

3 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

4 Implement emergency physical security procedures.

(b) Notification: Immediate supervisor, Information Systems Security Manager/Officer, Intelligence and Security Directorate, Provost Marshal (CID), FP Officer, and LIWA/ACERT.

(4) Activists (Outsider threat). Activists usually want to destroy or disrupt activities with which they disagree to bring notoriety to their cause and to embarrass those conducting the activity. Attacks are for the purpose of disruption, destruction, or gathering of information to use in obtaining their goals. The affected protection categories are: availability, confidentiality, and integrity.

(a) Countermeasures:

1 Restrict access to computer facility.

2 Implement emergency physical security procedures.

3 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

4 Review audit trail information to determine magnitude of damage and notify all data owners of possible data compromise.

5 Invoke contingency plan with essential backup software to restore operations.

(b) Notification: Immediate supervisor, Information Systems Security Manager/Officer, Intelligence and Security Directorate, Provost Marshal (CID), LIWA/ACERT.

(5) Industrial espionage (Outsider threat). Industrial espionage is the act of gathering proprietary data from one company for the purpose of aiding another company. A target within AMC would be any information with economic implications such as data related to patents and Cooperative Research and Development Agreements. The affected protection category is: confidentiality.

(a) Countermeasures:

1 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

2 Review audit trail information to determine magnitude of damage and notify all data owners of possible data compromise.

3 Implement network protection (filtering) to protect and control Internet Protocol (IP) addresses.

4 If necessary, invoke contingency plan with essential backup software to restore operations.

(b) Notification: Immediate supervisor, Information Systems Security Manager/Officer, Intelligence and Security Directorate, Provost Marshal (CID), and LIWA/ACERT.

(6) Disgruntled employee (Insider threat). This type of individual usually takes destructive actions to discredit the organization or damage its resources. Actions to achieve these results include introduction of malicious software to cause time delay damage to the AIS or data or theft of data for purposes of blackmail, embarrassment, or exposure. The affected protection categories are: availability, confidentiality, and integrity.

(a) Countermeasures:

1 Restrict access to computer facility.

2 Limit "root" access to data, data bases, and operating system to Systems Administrators only.

3 Maintain configuration control, and periodically verify the configuration (operational and security) established for the system.

4 Review audit trail information to determine magnitude of damage.

5 Review/reenforce procedural security standards.

6 Review personnel security requirements and remove employee access to AIS and associated media, if determined to be appropriate.

(b) Notification: Immediate supervisor, Provost Marshal, Civilian Personnel Office, Installation Systems Security Manager/Officer, and Intelligence and Security Directorate.

(7) Psychotic employee (Insider threat). This is a unpredictable threat to AMC AIS. Onset of damaging types of activity can begin gradually and accelerate over a period of time, or activity may be characterized as one dramatic outburst. Both motive and goals of any activity are usually without logic, although often aimed at retribution for imagined slights or injury. The affected protection categories are: availability, confidentiality, and integrity.

(a) Countermeasures:

1 Restrict access to computer facility.

2 Limit "root" access to data, data bases, and operating system to only Systems Administrators.

3 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

4 Review audit trail information to determine magnitude of damage.

5 Review/reenforce procedural security standards.

6 Review all data files to which employee had access to determine if any have been modified or destroyed.

7 Review personnel security requirements and remove employee access to AIS and associated media.

(b) Notification: Immediate supervisor, Provost Marshal, Civilian Personnel Office, Installation Systems Security Manager/Officer, FP Officer, and Intelligence and Security Directorate.

(8) Untrained or careless employees (Insider threat). These individuals pose two types of threats to AMC AIS. First, when employees fail to observe security rules or procedures designed to protect system resources and information, the system security is degraded. Secondly, carelessness or lack of training can result in damage to the system and alteration or destruction of data. The affected protection categories are: confidentiality, integrity and availability.

(a) Countermeasures:

1 Limit "root" access to data, data bases, and operating system to Systems Administrators only.

2 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

3 Review audit trail information to determine magnitude of damage.

4 Review/reenforce procedural security standards.

5 Review personnel security requirements and remove employee access to AIS and associated media, if determined to be appropriate.

(b) Notification: Immediate supervisor, Installation Systems Security Manager/Officer, FP Officer, and Security Manager.

(9) Criminal activity (Insider/Outsider threat): Criminal activity is primarily an insider threat resulting in the loss of resources. Information loss would be a byproduct of theft of equipment, which could be sold or held for ransom. The affected protection categories are: availability and confidentiality.

(a) Countermeasures:

1 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

2 Review audit trail information to determine what information may have been present on the AIS.

3 Notify all data owners of possible compromise of their data.

4 Implement damage control. Determine what physical security measures were not implemented which allowed employee to remove equipment from the work site.

5 Coordinate disciplinary actions with Command Counsel and Civilian Personnel Office.

(b) Notification: Immediate supervisor, Provost Marshal, Civilian Personnel Office, Information Systems Security Manager/Officer, and Security Manager.

(10) Environmental threats. Threats in this category relate primarily to natural events that can destroy, interrupt, or alter the normal functioning of facilities, equipment, and personnel. These events include fire, wind storms, flood, earthquakes, lightning, and snow or ice storms. The affected protection categories are: availability and integrity.

(a) Countermeasures:

1 Implement emergency physical security procedures.

2 Implement damage control.

3 Implement contingency plans.

4 Maintain configuration control and periodically verify the configuration (operational and security) established for the system.

(b) Notification: All employees and management.

5-12. Information assurance/C2 protect responsibilities.

a. The AMC Deputy Chief of Staff for Corporate Information (DCSCI) will function as proponent for the Command AIS Security Program. This includes identification of available training and proponency for the command AIS security budget.

b. The Civilian Personnel Advisory Center/Civilian Personnel Operations Center (CPAC/CPOC) will provide guidance on removal of personnel from sensitive computer positions and duties, as required.

c. The Information Systems Security Manager will oversee the execution of the AIS security program to include the training and awareness program; accreditation; threat and vulnerability assessments; reporting of AIS security incidents and technical vulnerabilities; and advising the local commander on appropriate security countermeasures to be implemented.

d. The Information Systems Security Officer, Network Security Officer, and Systems Administrator, will ensure systems within their purview are operated and maintained per applicable policies. They will--

(1) Ensure all critical computer positions have been properly coded for the required level of security investigation.

(2) Ensure users have the appropriate clearance, authorizations, and need-to-know.

(3) Review audit trails.

(4) Report AIS security incidents.

(5) Conduct user security awareness training.

e. The immediate supervisor will ensure all employees follow established security procedures.

f. Each employee will follow established security procedures and know the appropriate chain of command for notification of abnormal AIS activity and unusual co-worker behavior.

g. Outside agencies in the notification process for AIS security incidents include the Land Information Warfare Activity (LIWA), who when appropriate, will notify the Defense Information Systems Agency (DISA) for the reporting of suspected/actual unauthorized/hacker activity, and the local MI element if damage to sensitive/classified AIS and/or foreign involvement is suspected.

h. The Security Manager will report unfavorable personnel security-related information to the U.S. Army Central Personnel

Security Clearance Facility, Fort George G. Meade, MD, per Change 3 to DOD 5200.2R, Appendix I-17 - Misuse of Information Technology Systems.

5-13. Information assurance/C2 protect training.

a. Information Systems Security Manager training is available from DISA and DISC4. Classes are conducted monthly at various locations throughout the country. Tuition is free; travel is the responsibility of the student's home station.

b. Information Systems Security Officer training is available from DISA, DISC4 and from the DOD Security Institute in Richmond, VA. Training schedule varies, usually four classes per year. Tuition is free; travel is the responsibility of the student's home station. This training is also available via the mobile training team concept when sponsored by the requesting organization in coordination with Defense Security Service (DSS). The sponsoring organization provides the classroom space and pays the cost of the TDY of the instructors and course materials for each student.

c. Network Security Officer training and Systems Administrator training is available at Fort Gordon, GA and Computer based Training (CBT) is available through DISA.

5-14. Information assurance/C2 protect funding. a. MS4X (OMA) funding may be used for salaries, travel, training and oversight. Information Systems Security Managers will respond to AMC DCSI data calls for these resource needs.

b. MX5T (OPA) funding may be used for hardware, software site licenses, encryption products, and secure communications devices. Information Systems Security Managers will respond to AMC DCSI data calls for these security requirements.

c. VTER (Force Protection OMA) funding may be used for security products in support of Force Protection. Data calls and responsibility for input to AMCPE-S.

5-15. Information assurance/C2 protect oversight.

a. Installation Information Systems Security Managers will ensure that implemented security countermeasures are routinely tested to determine effectiveness. Audit trails will be regularly reviewed and user-id and password programs will be routinely tested for evidence of possible compromise.

b. The AMC Security Support Division will periodically inspect all AMC major subordinate activities and separate reporting activities as part of their Intelligence and Security Program Overview. Compliance with Information Assurance/C2 protect regulations and directives are items of interest on their inspection checklists.

5-16. Law enforcement activities. a. *General*. Law enforcement remains an integral element of the Command's Force Protection Plan (FPP). Comprehensive and aggressive law enforcement measures and services deter criminal as well as terrorist activity, and often represents AMC Installation Commanders' only immediate emergency response capability. The Provost Marshal is the proponent for law enforcement activities within AMC.

b. *Threat analysis*. Commanders will assess the adequacy of law enforcement measures and services during all phases of operational planning and execution. As a minimum, requirements for the following activities will be considered, and, as appropriate, integrated into current and future operations.

(1) Traffic Control Planning. Proper traffic control maximizes the safe and secure flow of vehicles with minimum control and direction. Traffic control planning includes the use of barriers, directional signals, pedestrian and motor vehicle control procedures, parking policies, and safety regulations. A traffic control plan will be developed and implemented for each AMC installation and, when appropriate, for each AMC contingency operation. Traffic control for civilian areas adjacent to AMC facilities will be coordinated with local law enforcement agencies.

(2) Military Police Management Information System (MPMIS). MPMIS is the Army's automated system for processing and maintaining law enforcement information. It reduces the administrative burden of information management on provost marshal staffs, and increases awareness of problem areas through statistical analysis. MPMIS applications with significant impact upon the AMC FPP include the Offense Reporting System (ORS-2), the Security Management System (SMS), and the Registration and Access Control System (RACS). Employment of the MPMIS in support of AMC law enforcement activities is mandatory, wherever possible.

(3) Special Reaction Teams (SRT). SRT are specially trained and equipped teams comprised of military or civilian law enforcement personnel who serve as the commander's principal response force in the event of a major incident or terrorist act. AMC installations should maintain an SRT, as required.

Operational planners will consider the need for SRT as part of all contingency operations.

(4) Military Working Dogs (MWD). Like other highly specialized items of equipment, MWDs complement and enhance a commander's security capabilities and posture. MWD teams provide both a law enforcement and physical security capability and serve as a strong psychological deterrent to potential offenders. All AMC MWD teams, except for the kennelmaster, will be dual capable

with their assigned MWD (either patrol/explosive or patrol/drug trained). All AMC MWD teams are subject to deployment. Operational planners will consider the need for MWD as part of the force protection package during all operational missions.

(5) Employment of Law Enforcement Personnel. Law enforcement personnel, whether military or civilian, may be employed to protect persons and/or property under a myriad of diverse circumstances. The employment of law enforcement personnel is among the most costly of force protection measures. Since they are most efficient and versatile when assigned to patrol missions, automated and remote intruder detection systems will be employed whenever possible to protect static posts or other fixed facilities. AMC law enforcement personnel may be subject to deployment. Operational and security planners will consider the need for law enforcement personnel as part of all force planning initiatives.

(6) Violence in the workplace. Stress in the work environment remains a major contributor to aggressive and often violent behavior in both the office and contingency environments. A leader's interpersonal and professional skills are important in recognizing and taking appropriate action to prevent such incidents. Commanders and operational planners must ensure recurring training of leaders in managing and recognizing stress in the workplace and on methods of responding to incidents of violence which threaten the work force. Planning to prevent and respond to violence in the workplace will be incorporated into all AMC activities and all force protection planning for contingency missions.

(7) Criminal Investigation and Criminal Threat Support. The U.S. Army Criminal Investigation Command (CID) provides criminal investigations support to the Army, and remains the proponent for acquiring and disseminating criminal threats to Army persons, facilities, equipment and operations. Commanders and operational planners will ensure regular coordination with local CID elements during all facets of routine activities, as well as all contingency operations.

c. *Reporting of incidents*. All major incidents or terrorist acts, whether actual or alleged, will be reported per AR 190-40, AR 525-15 and this regulation. The reporting of these incidents is mandatory.

5-17. Physical security. a. The AMC Physical Security Program (PSP) is a component of the FP program, and consists of policies, procedures, and responsibilities to deter, detect, and defeat threats to AMC soldiers, employees, facilities, assets, and operations. The Command Provost Marshal (CPM) serves as the AMC proponent for the PSP and exercises staff oversight of associated policies and resource development. Commanders implement the PSP, and, cognizant of associated and identified threats will--

(1) Identify and prioritize their assets.

(2) Survey facilities used to house and store those assets.

(3) Analyze and categorize the risks and vulnerabilities to identified assets.

(4) Plan and program adequate resources to protect those assets determined to be critical to the command or operation.

b. Physical security guidance/requirements are contained in AMC Supplements to AR 190-11, Physical Security of Arms, Ammunition, and Explosives, and AR 190-13, The Army Physical Security Program. Additional requirements are contained in AR 190-51, Security of Unclassified Army Property (Sensitive and Unsensitive) and DA PAM 190-51, Risk Analysis for Army Property.

c. Continuous analysis of the threat is essential to ensuring the effectiveness of the AMC PSP. Per AR 190-13, installation commanders, develop and maintain a local threat assessment upon which all physical security and force protection planning is based. In addition, operational planners will develop and include a threat assessment as an element of all contingency plans.

d. Threat assessments must include all reasonable criminal, intelligence, and terrorist threats known to exist. FBI, MI, CID, and local law enforcement agencies will be solicited to provide periodic updates. The Provost Marshal will be the focal point to receive and disseminate of all "time sensitive" threat information.

e. Commanders will develop and implement a physical security plan for all installations within the command. In addition, commanders and operational planners will ensure that physical security of AMC resources remains a required planning consideration in contingency operations. Physical security plans will be developed per FM 19-30 Physical Security, and will be included as an appendix to all Force Protection plans and/or annexes. Tabs to the physical security plan will include, as a minimum:

(1) Provisions for an installation threat statement.

(2) A terrorism counteraction plan.

(3) A bomb threat plan.

(4) An installation or base emergency closure plan.

(5) Natural disaster and civil disturbance plans coordinated with local authorities.

(6) A communications plan.

(7) A listing of all installation mission essential vulnerable areas (MEVA).

5-18. Physical security - risk analysis. Not all Army assets require the same degree of protection at all locations. The risk analysis process allows the commander to prioritize assets so that physical security resources can be applied in the most efficient and cost effective manner possible. Risk analysis indicates both the impact of the compromise of an asset and also evaluates the potential for it being compromised. Risk analysis will be conducted on MEVAs and whenever one of the following events and/or conditions are met:

a. A unit or activity is activated.

b. When a unit permanently relocates.

c. When determined that no previous record of risk analysis exists for a MEVA.

d. At least every 3 years.

e. During contingency planning stages.

f. During planning for a new, addition to, or renovation of facility.

g. Whenever an incident occurs in which assets are compromised.

5-19. Physical security - planning process. a. Installation provost marshals, security officers, and/or operational planners assess physical security requirements for installations and develop contingencies based upon the following:

(1) An operational risk analysis conducted per DA Pam 190-51.

(2) The mission to be accomplished.

(3) The threat (known and/or perceived).

(4) Mission Essential or Vulnerable Activities (MEVA) protection requirements.

(5) Findings of previous physical security surveys, if available.

(6) Availability of resources.

b. The following security measures will be considered in developing physical security plans:

(1) *Electronic Security Systems (ESS)*. Electronic Security Systems, if effectively utilized, decrease and eliminate requirements for fixed guard posts. An intrusion detection system (IDS), when installed, is classified as "personal property, equipment in place" and will be accountable by the using unit or activity. The Joint Services Interior Intrusion Detection System (J-SIIDS) is the DOD standard IDS. Initial issue of these systems is not charged to the installation. Repair or replacement parts/components of J-SIIDS are chargeable to the installation. Commercial Intrusion Detection Systems (CIDS) are funded under MDEP RJC6 (physical security). Closed Circuit Television (CCTV) should only be installed for interface with existing or planned IDS as an assessment device. CCTV should not be installed solely for surveillance purposes.

(2) *Structural Designs*. Commanders and operational planners must ensure incorporation of physical security measures into the structure designs of all facilities to include those erected as part of a contingency mission. Provisions must be made for storing arms, ammunition, and explosives, and for protecting facilities housing personnel and critical equipment and communications centers from explosions, vehicular ramming, and other forcible intrusions. Guidance and information for enhanced structural measures can be found in the U.S. Army Corps of Engineer Security Engineering Manual.

(3) *Perimeter Barriers*. Barrier protection is often an effective means of deterring and protecting against vehicular intrusions and explosions in the contingency environment. Where U.S. Army property requires fencing as a protective measure, the type and quantity of fencing will meet the requirements of U.S. Army Corps of Engineers' specifications. Other barriers such as bollards, walls, gates, berms, will be considered and constructed, as needed.

(4) *Access Controls*. Commanders and operational planners will designate areas or facilities subject to special restrictions or security controls prior to commencement of operations. Three types, or levels, of restricted areas are used: Exclusion Area, open to only those personnel required to have access; Limited Area, open to personnel may have access with an authorized escort; and Controlled Area, open to personnel may have unescorted access. A limited access installation or activity may be designated under specific criteria; no perimeter fence exists but entry can be temporarily closed to vehicular traffic; or permanent barriers exist and access is controlled only after normal duty hours, i.e., gates are secured or manned after dark; or no permanent barriers exist, but vehicular traffic and other movements using roads and other points of entry are continuously controlled.

(5) *Transportation Security*. Commanders and operational planners will consider and include security requirements for the

transport of AMC equipment (arms, ammunition, and explosives) and personnel during all phases of deployment and/or contingency operations.

(6) *Physical Security Surveys*. The Provost Marshal directs physical security surveys of all commands and separate activities within AMC per AR 190-13 and AMC Supplement 1. In addition to conducting compliance inspections and surveys, Provost Marshal physical security inspectors are trained to identify and report physical security vulnerabilities not provided for in existing regulation or policy. Commander and operational commanders are encouraged to coordinate for physical security survey support at the outset of a contingency operation.

5-20. Personal security. a. *General*. Personal security operations in AMC include those measures taken to identify, train, and prevent an attack upon a member of the Command, to include formal protective service operations undertaken to protect select high risk personnel. The Provost Marshal remains the proponent for Personal Security within the AMC.

b. *Designation of high-risk personnel*. The CG, AMC retains the authority to designate high-risk personnel within the Command. High risk personnel are those who are more likely to be terrorist or criminal targets because of their grade, assignment, symbolic value, vulnerability, location, or specific threat. Commanders and operational planners will review the permanent assignment, projected temporary duty, and deployment of all AMC personnel and contractors for consideration of designation as a high risk on an annual basis and during contingency planning. There are two categories of high-risk personnel:

(1) Level 1. Level 1 personnel have such a significantly high potential as terrorist or criminal targets as to warrant exceptional security measures to include assignment of full-time protective services. This would include long-term protective services based on assignment location, or short-term protective service based on a specific threat.

(2) Level 2. Level 2 personnel do not warrant assignment of full-time protective services but require such additional office, residential, and travel security measures as deemed appropriate based on local conditions.

c. *Personnel security measures*.

(1) Commanders with subordinate personnel permanently assigned OCONUS will ensure coordination with the sponsoring OCONUS commander to ensure appropriate security measures are in place. AMC commanders will ensure that AMC personnel are properly trained, routinely provided local threat information, and afforded adequate security protections.

(2) Commanders will annually review the need for personal protective equipment and evasive driving training for all personnel assigned to high risk OCONUS areas.

(3) Commanders will review and determine the need for personal protective equipment and evasive driving training for all personnel who will travel in high risk OCONUS areas for a period of 30 days or more.

d. *Protective services*.

(1) Protective service operations are a means of protecting high-risk personnel. The mission of protective services is to protect the principal from assassination, kidnapping, injury, and embarrassment. Protective service operations will be conducted per U.S. laws and regulations, and international agreements to which the U.S. is a party. Conduct of protective services, organization of the protective service force, the number of personnel employed, and the duration of the mission will be determined based on the status of the principal, threat, vulnerabilities, location, and other conditions that may present a danger to the principal being secured.

(2) Commanders and operational planners must consider all means available for protecting high-risk personnel when conducting routine operations and planning contingencies. Protective services remains a very costly security measure and should be employed only for Level 1 designated personnel and only under the most critical circumstances. Other technological measures to include personal protective equipment and remote surveillance devices should be considered as a means less intrusive than a protective services detail.

e. *Protective service details*. The objectives of the protective service detail are--

(1) Deter possible harm to the principal through protective service operations.

(2) Detect threatening situations affecting the personal safety and security of the principal.

(3) Defend the principal from physical harm or embarrassing situations.

(4) Quickly and safely remove the principal from the threatening environment

5-21. Intelligence support. a. *General*. Every AMC element/employee has a responsibility and a role in the Force Protection Program, both as a player (contributor) and as a customer (user). In order for AMC FP elements to effectively carry out their designated responsibilities in the FP area, and to

protect themselves and decrease their risk of an incident, the proper use and dissemination of intelligence information is critical.

b. *Objective*. All AMC FP players/customers must be--

(1) Identified, (with roles/responsibilities defined).

(2) Trained.

(3) Properly resourced.

(4) Supported with all-source and timely intelligence.

c. *Concept*. To successfully execute the command FP mission, the following intelligence support tasks must be accomplished:

(1) Identify command FP customers/players.

(2) Identify command FP requirements.

(3) Establish valid command FP requirements.

(4) Collect and tailor information.

(5) Disseminate information.

(6) Provide oversight/feedback mechanisms.

d. *Responsibilities*.

(1) AMC Deputy Chief of Staff for Intelligence (DCSINT). The AMC DCSINT, as the Command Senior Intelligence Officer (SIO), will--

(a) Provide policy, guidance and technical assistance commandwide to ensure proper intelligence is available and accessible in support of AMC's Force Protection Plan (FPP) and to combat threat programs/personnel.

(b) Serve as focal point for all requests for foreign threat information dealing with Force Protection issues.

(NOTE: The collection or gathering of information on U.S. citizens by DOD Intelligence organizations or Intelligence-related activities is strictly forbidden under AR 381-10, Intelligence Activities. The PM is the command element that acts as the liaison between local law enforcement entities and AMC for this type of information.)

(c) Coordinate with local supporting military intelligence units, on-line national and DOD elements, and Command Provost Marshal for current threat information.

(d) Disseminate threat information to AMC FP customers and players.

(e) Working with the AMC FP Officer, ensure threat information pertinent to personnel traveling OCONUS is incorporated into the Level I AT/FP travel briefing.

(f) Working with the AMC FP Officer, ensure accurate and valid threat information is contained in FP-related training and information briefings within AMC commandwide.

(g) Provide intelligence support to MSC Force Protection Officer (FPO), Senior Intelligence Officer (SIO), Foreign Intelligence Office/Officer (FIO), Security Manager/Office (SM), and Provost Marshal (PM), as required.

(h) Prepare and update the annual HQ AMC threat assessment and ensure it is available commandwide for use by commanders/directors as a reference during the creation of their own organizational threat assessments.

(i) Provide MACOM program management for QSEC and GP3I MDEPs in support of command FP. Identify intelligence support resource shortfalls; prioritize and submit unfinanced requirements (UFR) and/or resource submissions through the Program Objective Memorandum (POM) cycle.

(2) AMC major subordinate command (MSC) commander. AMC MSC commanders will ensure their command implements the AMC FP intelligence support functions. Typically, a Senior Intelligence Officer (SIO) is designated at each MSC and is responsible for executing the intelligence support functions to the AMC FPP. In cases where a SIO does not exist or has not been designated by the local commander, the Security Manager (SM) will normally be designated to perform the intelligence support functions/duties discussed in this regulation.

(3) Senior Intelligence Officer (SIO). The AMC MSC Senior Intelligence Officer (usually the head of a joint Intelligence and Security division/directorate) will ensure both intelligence and security support to FP operations occurs. At the AMC MSC level, this responsibility usually falls on the command Foreign Intelligence Office/Officer (FIO) and/or the Security Manager (SM). In conjunction with the FIO/SM and PM, establish a "feedback" mechanism to ensure that intelligence information/training provided to the command is relevant and has been received in a timely fashion.

(4) Foreign Intelligence Office/Officer (FIO). The AMC Foreign Intelligence Office/Officer is responsible for providing all-source intelligence support to appropriate command elements (Security Manager, Provost Marshal, Operations Center, etc.) in support of command FP. The FIO will--

(a) Identify local command FP customers/players.

(b) As a member of the command FP team, assist in identifying specific threats to local command.

(c) Identify and register valid local command FP requirements.

(d) Collect and analyze FP data/information produced based on command requirements.

(e) Disseminate threat information to command customers.

(f) Execute command feedback/oversight mechanisms.

(g) Working with the PM/SM MSC CDR and Resource Management (RM) personnel, identify intelligence support resource shortfalls within the command; prepare UFRs, Program Objective Memorandum (POM) submissions; forward through command channels for validation/adjudication.

(5) Security Manager/Office. The Security Manager/Office (SM) is a key link in the command FPP. Working in conjunction with the FP Officer, PM and FIO, the SM will--

(a) Assist in identifying local command FP customers and their requirements.

(b) Assist in identifying specific threats to local command.

(c) Disseminate threat information to FP customers.

(d) When so designated, serve as the focal point for all intelligence support to FP in the absence of a SIO at the MSC (and below) command level.

(e) Working with the FP Officer, PM/FIO, MSC CDR and RM personnel, ensure proper intelligence resources are available to support command FPP implementation and execution. Identify and forward intelligence UFRs/POM submissions and intelligence related FP training requirements through command channels for approval/adjudication.

(f) Closely monitor and evaluate SM intelligence/ security functions in support of AMC FP programs at AMC subordinate commands and installations.

e. *Intelligence requirements generation*.

(1) AMC DCSINT FP Representative. All requirements for intelligence information from HQ AMC elements in support of FP will go to the DCSINT FP representative for action. The office

symbol is AMXMI-SCM, room 1E22, ext 617-9066. Before submitting an intelligence requirement, the HQ AMC customer should review request and ensure the following information has been provided:

(a) When is information needed? If the information is critical to current/ongoing operations and is needed in a quick-reaction mode, so state. If the information is needed to complete long-term FP plans/projects, be sensitive to when the information is actually needed (information should not be requested under a quick-reaction mode if it can be delivered at a later acceptable date with no impact to AMC FP). This ensures that proper Intelligence Community resources are tasked against AMC requirements.

(b) Has the total requirement been stated and will it be understood? One of the responsibilities of the AMC DCSINT is to work with the customer to ensure that the requirement is valid and the customer is asking for the right information.

(2) AMC DCSINT Requirements Manager is responsible for the validation and submission of intelligence requirements in support of FP. The Requirements Manager works closely with the AMC DCSINT FPO to ensure command FP requirements are submitted and tracked to completion. If questions as to the status of a FP intelligence requirement arise, and the AMC DCSINT FPO is unavailable, the Requirements Manager may be contacted for status of the requirement. The office symbol is AMXMI-INT, room 1S58, ext 617-5275.

(3) AMC MSC (and below) level:

(a) At AMC elements where there exists both an FIO and SM, the FIO will be the focal point for all threat-related FP requirements and the SM will be the focal point for all FP countermeasure requirements. Coordination between the FIO and SM on all command FP requirements is essential before the command requirements manager forwards for action.

(b) With the introduction of automated systems linked to data bases in the intelligence community, the ability to research information at the local level exists. If, after searching available intelligence sources the information requested is not available, an intelligence gap has been identified and the following steps will be followed:

1 The FIO will determine if requirement is quick-reaction (QRR, needed in 1-10 days) or Request for Information (RFI, needed in 11-45 days). If an involved area assessment needs to be done, this may require a long-term assessment which would require a Production Requirement (PR, 45 days and longer) to produce.

2 If it is a QRR, submit requirement directly to appropriate intelligence element (Army, U.S. Army National Ground Intelligence Center (NGIC), ATTN: IANG-PO). Info copies will be forwarded to HQ AMC, ATTN: AMXMI-SCM/AMXMI-INT and to HQDA, ATTN: DAMI-CHS. Requirement should contain information needed, (with justification for the short suspense), suspense date, and point of contact (POC) (both customer and intelligence representative). Media for delivery (FAX, STU-III, Genser msg, unclassified e-mail, classified e-mail CIPRNET/INTELINK-S or INTELINK) should be included.

3 If RFI, submit requirement just like a QRR above. HQ AMC (AMXMI-INT) will ensure the RFI is linked to existing PR and forward to Production Center.

4 If a detailed recurring FP intelligence requirement exists (one that requires extensive information in final product form), a PR will be generated by intelligence/ security personnel and forwarded through Command channels for tasking. Within AMC, PRs will be submitted to HQ AMC, ATTN: AMXMI-INT/AMXMI-SCM for validation. AMC ODCSINT will forward requirement to appropriate Production Center for resolution.

5 FP intelligence requirements will be reviewed at the MSC level annually to ensure they are current, valid, need to be updated, or canceled.

f. *Analysis and dissemination of AMC FP intelligence information.*

(1) Once information has been collected in support of an AMC FP requirement, it will be analyzed to determine applicability to AMC FP mission and then tailored to meet the need. Results of analysis will be coordinated with the AMC FP Officer and appropriate AMC FP Working Group members before dissemination occurs (when possible).

(2) The AMC ODCSINT has established Automated Information Group (AIG) 11557. The purpose of this AIG is to disseminate Force Protection information with impact on AMC to AMC elements.

(3) At the AMC MSC level, the AMC Senior Intelligence Officer (SIO) will ensure that pertinent FP information is disseminated in a timely fashion. Procedures and processes involved with the dissemination of FP information will be the responsibility of the SIO.

(4) Established FP information dissemination procedures/ processes will be reviewed during periodic security inspections/ staff assistance visits for compliance/effectiveness.

(5) With the advent of accessible automated data bases (intelligence and nonintelligence) as a source of information, a

more timely response to customer FP needs can be achieved. FIOs/SMs will conduct searches of Intelligence Community automated data base files for both information sources and information that responds to their requirements. AMC MSC Intelligence and Security (I&S) elements (located in or having access to Sensitive Compartment Information Facilities (SCIF)) will have access to INTELINK by the first quarter fiscal year 1998. INTELINK is DOD's classified "INTERNET" and provides I&S personnel a means of accessing near real-time FP information. Examples of FP information available on INTELINK are JCS Morning Brief (daily), DIA Terrorist Summary (daily), and CINC daily INTSUMs (includes terrorist update).

(6) Other sources of information include HQDA Force Protection Travel Advisory (quarterly), HQDA Force Protection Message (daily), Monthly International Terrorism Summary (monthly), Secretary of State Travel Advisories/Consular Notes (periodic), AMC Threat Statement (updated annually), Defensive Security Briefings, Provost Marshal - for relevant law enforcement information.

(7) AMC MSC I&S personnel will ensure that their command's Statement of Intelligence Interest (SII) is current and reflects a need for FP information.

g. *Oversight*.

(1) Oversight management and feedback mechanisms are important vehicles to ensure the adequacy/relevancy of FP information (provided by AMC Intelligence and Security (I&S) personnel) and to gauge customer satisfaction. To ensure FP information is adequate/relevant and timely, feedback mechanisms must be initiated and institutionalized by AMC MSCs. Due to different and unique missions within AMC subordinate commands, a set format and/or criteria for feedback does not exist. It is incumbent upon the local I&S element to create a feedback system to evaluate the effectiveness of the information and service provided.

(2) All AMC I&S elements will review AIGs associated with intelligence support to FP semiannually to ensure distribution lists (customer base) are current.

(3) HQ AMC will review Intelligence Support to FP to ensure proper oversight and feedback mechanisms exist during scheduled Staff Assistance Visits (SAV) and during annual security inspections.

h. *Reporting of suspicious activity*.

(1) "Terrorism is a form of political communication. Violence is used to send a message. Violent acts are usually preceded by nonviolent or less than violent messages, i.e., written, spoken or physical action. These early messages of

protest, of changes in attitude leading to violence, as well as the observable preparations for a violent attack...all can provide early warnings of a coming attack, if we are alert, observe, and report." (R.D. Crelinsten)

The *Terrorist Operational Cycle* may follow a 7-step process.

1 - Target selection (by type).
2 - Initial surveillance by nonprofessionals.
3 - Planning.
4 - Final target selection.
5 - Deploy to target area/equip people.
6 - Final surveillance by professionals.
7 - Attack.

(2) AMC personnel can help to protect AMC's personnel, information, and activities by reporting certain activities, which could be observed during this cycle. Although a terrorist attack on an AMC activity is assessed as unlikely, we must remain alert to suspicious activity. Following simple security measures serves as the best deterrent to a terrorist act. Look for and report any of the following "potential indicators" to your nearest Military Police/Security Office.

(3) Report the following suspicious activity:

(a) Signs, speeches, or conversations which suggest violence towards established authority, leaders, ethnic, or political groups.

(b) Information that members of local organized groups are quitting or being expelled as "not fitting in."

(c) Persons emotionally expressing threats of violence toward individuals, groups, or institutions.

(d) Persons emotionally expressing feelings of being under attack, harassed or targeted by some other group or person.

(e) Persons emotionally or repeatedly blaming "others" for some problem and advocating violence as a solution to the problem.

(f) Multiple off-post thefts of funds, firearms, or explosives.

(g) A stranger loitering and suspiciously observing government buildings, people, or activities.

(h) A stranger asking unusual, personal, or detailed questions regarding AMC personnel, AMC building, and/or activities.

(i) A person taking pictures or making sketches of personnel and/or the building.

(j) An unusual, oversized, or inappropriately parked vehicle (particularly in the vicinity of large numbers of people or special events).

(k) Abandoned parcel or suitcase.

(l) Suspicious, oversized or unusual mail.

(4) When a suspicious activity is observed, the activity should be reported, containing as many of the following information elements as possible:

(a) Describe any people observed, i.e., name, sex, age, appearance, clothes.

(b) Provide time of day activity was observed.

(c) Describe location of activity.

(d) Describe type of vehicle, i.e., type, color, distinguishing marks, license plate.

(e) Describe package, suitcase, or mail, i.e., type, color, size, distinguishing marks.

(f) Describe the nature/details of any conversations or messages.

(g) Provide copies of any flyers, pamphlets, or messages which can be obtained without personal risk or exposure.

Report any suspicious activity immediately to--

Provost Marshal or security officer
Within HQ AMC, call: 617-9367 (duty hours)

Staff Duty Officer
Within HQ AMC, call: 617-9223 (after duty hours)

(5) Subversion and Espionage Directed Against the U.S. Army (SAEDA). Reportable SAEDA Incidents are--

(a) Attempts by unauthorized persons to obtain classified or unclassified information concerning U.S. Army facilities, activities, personnel, technology, or materiel.

(b) Attempts by individuals with known or suspected espionage, subversion, or foreign intelligence background or

associations to cultivate friendship with military and civilian personnel for the purpose of obtaining information.

(c) Any known, suspected, or possible unauthorized disclosure or deliberate compromise of classified information regardless of the circumstances.

(d) Active attempts to encourage military or civilian employees to violate laws, disobey lawful orders or regulations, or disrupt military activities (subversion).

(e) Known, suspected, or attempted intrusions into classified or unclassified automated information systems by unauthorized users.

(f) Any situation involving coercion, influence, or pressure brought to bear on DA personnel through family members residing in foreign countries.

(g) Actual or attempted suicide by any DA personnel who have had access to classified information within 1 year of the incident.

(h) Absent Without Leave (AWOL) DA personnel who have had access to classified information.

(i) Communications Security (COMSEC) violations except those concerning obvious administrative error.

(k) Persons having excessive knowledge or undue interest of sensitive Army facilities or operations.

Report suspicious activity involving SAEDA immediately to supporting counterintelligence (902d MI Group) element or local security manager.

Within the National Capital Region call--

(Commercial) 703-805-3008
(DSN) 655-3008

5-22. Resource/funding. a. During programming of contingency operations, commanders and operational planners will project and document force protection resource requirements as part of the overall cost of the operation. On an annual basis, installation level program managers will develop and prioritize a list of resource requirements to be funded under each appropriate Management Decision Packages (MDEP).

b. The operational planners and installation program managers will provide the resource requirements to the designated AMC program manager. The AMC program manager will review and validate program requirements. Validated requirements will be submitted in

the AMC Program Objective Memorandum (POM) process for funding consideration at Department of the Army.

c. *Executing FP funding*.

(1) Upon receipt of DA funding guidance for the next fiscal year, the AMC program manager will develop a distribution recommendation. The distribution recommendation will be used as a basis for Deputy Chief of Staff for Resource Management (DCSRM) to provide funding guidance to the installations.

(2) Once installations are in receipt of funding guidance, the Installation Resource Manager will notify the appropriate program manager of the target funding level. Executing a target based budgeting (TBB) action, the program manager will develop the resource plan based on the list of FP priorities. Resource requirements that cannot be funded within the provided target will be identified to the installation Resource Manager and the MACOM program manager as unfunded requirements (UFR).

(3) Installation program managers (or a designated representative senior to them) will participate in the Installation Process Budget Advisory Committee (PBAC) process. The purpose of participation in this forum is to defend existing funding against reprogramming to other priorities and to seek support for unfunded requirements.

(4) During the execution year, the AMC Program Manager will provide oversight of the MDEP execution. The Program Manager will be prepared to identify any reprogramming of FP funding and provide frequent updates to the AMC FP Committee and Command Group.

(5) History of requirements, resources, and subsequent execution will be maintained by the AMC Program Managers to be used as a factor in determination of future resource allocations.

d. *Description of MDEPS*. Force protection requirements may be included throughout the entire scope of MDEPS to include medical, engineering housing, etc. Funding provided in the following MDEPS are designed to improve the physical security of AMC installations and facilities or protect mission essential information that might be used to plan a terrorist attack.

(1) The VTER (antiterrorism) MDEP provides resources to protect all personnel (soldiers, civilian employees, and family members), equipment, facilities and information assigned to an Army installation against espionage, sabotage, and theft. VTER OMA funds can be used for personnel salaries, mission and training cost, and equipment costing less than $100,000. VTER OMA funds are 1-year funds and sent to the MACOM for disbursement to installations. Antiterrorism (AT) training classes at

Ft McClellan, Ft Huachuca, and Ft Bragg are funded with VTER OMA. VTER OMA can also be used to fund installation AT training cost. VTER OPA3 is 3-year procurement funds managed by HQDA and dispatched by the Physical Security Management Office (PSEMO) directly to the installation. Examples of VTER purchases include--

(a) *Closed circuit televisions (CCTV).

(b) *Intrusion detection systems/access control systems.

(c) *Secure communication equipment.

(d) Explosive detectors.

(e) Portable barriers.

(f) Security upgrades/hardening of mission essential vulnerable areas (MEVA), general officer (GO) quarters, and emergency operation centers.

(g) Special reaction teams (SRT) vans and equipment.

(h) Riot control equipment.

**** Requires additional funding for site-survey/preparation***.

(2) The RJC6 (Physical Security) OPA3 MDEP funds physical security equipment design, research, and development, test and evaluation, and procurement, installation, and maintenance of select physical security equipment and systems, to include intrusion detection systems and alarm monitoring systems. Physical security systems enhance security for nuclear and chemical storage facilities; sensitive arms, ammunition and explosive storage; mission essential and critical facilities; and equipment and personnel protecting against terrorism, espionage, and theft. Examples of RJC6 supported expenditures are--

(a) *Intrusion Detection Systems (ICIDS, J-SIIDS, Alarm Monitor Group (AMG)).

(b) *Sensors and Entry Control Systems.

(c) *Alarm displays.

(d) *Electronic Data Links.

(e) *Monitors.

(f) *CCTVs.

(g) Mobile Detection Assessment Response System (MDARS).

**** Requires additional funding for site-survey/preparation.***

(3) The QSEC (Director of Security) OMA MDEP funds personnel engaged in programs designed to protect the commands mission essential information. Information such as arrival and departure times for unit movements, operation plans, and administrative and logistical support arrangements are of particular value to terrorist. Denying the terrorist access to this information limits his/her targeting capability. Personnel funded with this MDEP are routinely involved in personnel security clearance processing, information classification and protection, information systems security (ISS), foreign visit and technology transfer programs, sensitive compartmented information and communications security.

(4) The MS4X OMA MDEP funds security enhancements for automated information systems. In some cases this decision package may be used to fund personnel engaged in ISS activities. Typical expenditures include ISS training for personnel who operate computer systems and hardware/software enhancements that provide protection against cyber-terrorism, hackers and virus infections.

(5) The QLPR (Security Law Enforcement) OMA MDEP provides resources for physical security, protective services, and law enforcement support to Army installations and facilities to maintain order, enforce laws and regulations, control vehicular and pedestrian traffic, protect critical government property and facilities, and investigate crimes. Operating account for Provost Marshal BASOPS activities (operations, civilian pay, contracts, training, supplies and equipment, special investigative tools, TDY travel, Military Working Dog Program, and pretrial confinement).

e. Fund cites should include an MDEP designation in the character string. If an improper MDEP is listed, an under obligation in the correct MDEP and an over obligation in the incorrect MDEP will occur. For this reason, it is extremely important that PM, RDA and RM counterparts monitor their obligation rates closely.

f. A concerted effort will be made by RM, PM or RDA counterparts to identify any Program Objective Memorandum (POM) Schedule 8 reprogramming action that affects FP requirements. Any proposed action will be identified to the FP Working Group, regardless of appropriation. Timely notification will enable the committee to defend and justify FP requirements.

g. Consistent with POM development timelines, resource managers will annually review all MDEP POM submissions to identify those which include FP requirements. All such requirements will

be consolidated and forwarded to the FP Officer for review by the FP committee to ensure proper categorization and nonduplication.

5-23. Engineering. a. Engineering provides guidance for use at all levels of command within AMC in project development to establish and implement criteria for protecting assets within facilities against a range of criminal, protester, terrorist, and subversive threats. The purpose of the guidance is to develop appropriate, effective, unobtrusive, and economical protective designs to a level appropriate for project programming. Commanders and operational planners must ensure incorporation of physical security measures into the designs of all facilities to include those erected as part of a contingency mission. Critical force protection considerations include (but are not limited to: stand-off distances from critical or heavily protected facilities; blast protection, intrusion detection, electronic surveillance measures, and emergency notification and evacuation requirements.

b. *Planning phase*.

(1) PLANNING TEAM - ORGANIZATION. The installation planning team must include, as a minimum, representatives of the facility users and the installation functions of intelligence, operations, security, logistics, environment, safety staff, and engineering. Other organizations such as the fire marshal and communications officer will be included as necessary. Specific responsibilities of the seven key planning team members relative to the planning phase are detailed below.

(a) Facility users. The ultimate users of planned/existing facilities identify the assets within the installation, which will require protection and establish their relative value. The users also identify any special operational or logistical design constraints for the facility.

(b) Intelligence. Representatives of this function are responsible for providing input for the identification of threats to identified assets including information on potential aggressors, their likely targets, and their likely tactics.

(c) Operations. Representatives of this function also serve as installation user representatives and are responsible for operational aspects of installation activities, including terrorism counteraction.

(d) Security. Representatives of the security and law enforcement function are responsible for detecting and defeating acts of aggression against assets. Therefore, these representatives supply information about the response capabilities of military police, contract or security guards, local police, or other applicable security forces. They also provide information on criminal threats.

(e) Logistics. Representatives of this function are responsible for maintenance of installed equipment in facilities. They provide input on equipment maintenance and on integrating with existing systems.

(f) Engineering. Representatives of this function are responsible for facility planning, construction, maintenance and repair. The Director of Public Works' organization includes the programmer. The programmer organizes and leads the planning team, develops a programming level protective design, and consolidates all facility requirements, design criteria, and project cost information into the appropriate programming document.

(g) Safety staff. Representatives of this function are responsible for integrating safety and risk management in all phases of the plan. They are responsible for identifying hazards; assessing hazards and risk in terms of probability and severity; developing countermeasures to eliminate hazards; implementing controls, and evaluating their effectiveness.

(h) Environment. Representatives of this function are responsible for conducting appropriate environmental inventories, consultations, and analyses to adequately address impacts of site selection on endangered species habitats, historic sites, archaeological significant areas, wetlands, or floodplain. Determine if project site is free from pollutants contaminants, and ordnance and explosive waste that would impact start of construction.

(2) PLANNING TEAM - OBJECTIVE. The objective of this phase of the force protection security engineering design process is to define protective system design criteria. The criteria describes assets associated with a facility, the threat to the assets, the level to which the assets are to be protected against the threat, and any constraints to the protective system design. The team must consider how security fits into the total project design and give it appropriate emphasis. Protecting individual assets is generally more cost effective than protecting an entire facility. Design criteria components are as listed below:

(a) Identification of all assets which are to be housed in the facility or facilities or which are a part of the project.

(b) Identify threats to each identified asset.

(c) Identify level of protection for the assets against the threats.

(d) Establish design constraints for the project.

c. *Programming phase - objective*. The objective of the programming phase of the force protection design process is to identify the appropriate protective measures for proposed construction projects which have a significant impact on the

project cost. This guidance is applicable to new facilities and to alterations of and additions to existing facilities. The programming procedure is summarized in the following steps:

(1) Step 1 - Select Protective Measures. These strategies help the programmer determine appropriate and necessary protective measures.

(2) Step 2 - Assess Design Opportunities and Constraints. Opportunities enhance protection, reduce requirements for protective measures, or solve a design problem resulting in an overall saving of time, design effort, or money. Constraints restrict design or create additional problems which must be compensated for by the protective design. Protective measures for one tactic may be opportunities or constraints to another.

(3) Step 3 - Determine required protective measures. Select required protective measures separately for each asset and each applicable tactic.

(4) Step 4 - Integrate protective measures into a protective system. To ensure uniform and effective protection of all assets against all threats, protective measures must be integrated into a system.

(5) Step 5 - Estimate protective system cost. Develop a programming level cost.

(6) Step 6 - Assess protective system acceptability. Acceptability depends on the system's cost effectiveness, its impact on operations, and its compliance with the design criteria established in the planning phase.

(7) Step 7 - Prepare documentation. Prepare required documentation for the type of project being programmed (DD Form 1391).

(8) Step 8 - Submit to the MSC a prioritized list of MCA, PAA and OPA3 funded force protection projects, required to protect the critical assets. RPMA, K and L account projects will be approved at the MSC level. MSCs will consolidate the installations MCA, PAA and OPA3 list, prioritize and submit list to AMC, ATTN: AMCEN-F.

d. *Project review*. AMCEN-F, at the appropriate time, will assemble the AMC Military Construction Working Group (MCWG) to review the MSC project submissions. Following the review, the MCWG will develop a recommended AMC priority list of MCA, PAA and OPA3 funded projects; the AMC Protective Forces Construction Program. Upon approval of the Chief of Staff, the Construction Program will be submitted to HQDA, DAIM-FDR for approval and funding.

5-24. **Public affairs**. a. Public Affairs Officers (PAO) will aggressively support command efforts to protect the Army from terrorist or criminal attack by ensuring an accurate, timely, and rapid flow of information from the command to internal and external audiences.

b. Public Affairs (PA) programs will support command efforts to increase the awareness of the Total Army family about the local criminal and terrorist threat, and supplement or support personal protection and Force Protection training programs.

c. Public Affairs Officers will work closely with Operations and Security elements to meet the information needs of all audiences without violating OPSEC.

d. *Concept of operations*.

(1) General. Each aspect of the U.S. Army Force Protection effort -- Physical Security, Combating Terrorism, Law Enforcement Operations, Information Operations, and Personal Security -- will be addressed by effectively using the three main components of Public Affairs: Command Information, Community Relations and Public Communications. Force Protection Public Affairs will be centrally coordinated, with decentralized execution at the MSC/SRA/subelement levels. DOD, HQDA and HQ AMC will provide information, guidance, announcements and messages for inclusion in on-going information campaign.

(2) Implementation.

(a) Major subordinate command PAOs will prepare, staff, coordinate and implement a Force Protection Public Affairs Plan per this annex, cited references and such Public Affairs guidance as shall be provided. The PA Plan must support the Commander’s Force Protection Plan to ensure there is a timely flow of critical information to all members of the local Army community and to meet the needs of the news media. Key elements that must be included in the plan are--

1 The role of the PAO in the Emergency Operations Center (EOC).

2 Location and resources for a media center.

3 How to control media access in the event of an incident.

4 The establishment of photography and other ground rules.

5 How to conduct the internal information program.

(b) During normal situations, Public Affairs assets at all levels will--

1 Conduct an active and sustained Command Information effort, using multimedia methods to help maintain general Force Protection and situational awareness for internal audiences. Provide timely information on personal countermeasures and the THREATCON system. The Command Information effort is to execute and supplement existing or future DOD, DA and AMC programs.

2 Help raise awareness of the Army Family to potential Force Protection issues and criminal or terrorist acts: soldiers, reservists, civilian employees and their families, as appropriate.

3 Provide accurate and timely information to minimize speculation and dispel rumors.

4 Instill confidence that the Department of Defense and the Army can reduce vulnerability of personnel, property and equipment, and protect itself from potential threats.

5 Provide timely and accurate Public Affairs guidance to supplement Force Protection messages.

(c) During an actual or potential criminal or terrorist incident, Public Affairs assets at all levels will--

1 Keep audiences informed, while at the same time, avoiding the image that the command is under siege. The presentation of such an image will further the potential terrorist or criminal goal of creating fear and confusion.

2 Coordinate release of materials with appropriate agencies (AMC, DA and DOD) prior to release. Ensure print, photo, and multimedia products are available for all to provide a seamless exchange of information and ensure all are addressing the same messages.

3 Provide on-scene Public Affairs support as requested or directed by competent authority.

4 Support the commander by releasing specific, approved information regarding force safety or the use of security forces.

5 Provide accurate and timely information, approved for release, to the news media to minimize speculation and dispel the inevitable rumors, which spread.

6 Prevent terrorists from using Army assets to manipulate the media and achieve their goals of massive publicity.

7 Prevent members of the media from interfering with or influencing military responses.

8 Prevent information about the preparation and deployment of military and law enforcement forces from being released through Army Public Affairs channels.

9 Ensure, to the maximum extent possible, that all official Army information originates from a single authorized approving source, thereby reducing the possibility of compromising key information and of releasing conflicting or inconsistent information.

10 Stress military-civilian police and governmental cooperation and joint efforts to deal with the situation.

(3) Coordinating Instructions.

(a) Release Authority.

1 AMC Commanding General and his/her designated representative, the AMC Chief of Public Affairs, are the release authorities for matters under the provisions of this plan and annex.

2 Release authority may be further delegated, as needed, by the AMC Commanding General and his/her designated representative, the AMC Chief of Public Affairs.

(b) Restrictions.

1 Per existing HQDA PAG, all requests to film, interview, photograph or record counterterrorist training, personnel, or units will not be approved.

2 Do not allow news media or any other unauthorized person access to classified information, materials, photographs or documents. Classified material, documents and information must be protected at the source and per AR 380-5.

3 THREATCON status and safety measures are For Official Use Only (FOUO) information. Force Protection messages will not be released, posted or distributed to internal or external media without proper command authorization.

4 When commands have declared a THREATCON, command information programs should be used to keep internal audiences informed about actions being taken and the reason for those actions. Internal information programs also reinforce the requirements to maintain OPSEC, keep the personnel informed of safety measures they should take, and help minimize rumors.

5 PA personnel and elements at all levels will participate in and support all training under the provisions of this plan. These training events will prepare PA personnel and elements to better respond to actual emergency situations. Training exercises provide the PAO the opportunity to solidify the PAO role as a critical member of the military team and to demonstrate how an effective PA operation can support the mission.

5-25. Legal support. a. *General*. At their respective levels (major command, major subordinate command, installation, unit), legal offices and personnel provide legal support to AMC commanders and staffs on all aspects of force protection planning and operations. All planning and operations will conform to the requirements of the applicable laws, directives, regulations, and other authoritative policy documents.

b. *Execution*. Commanders will ensure that their supporting legal officers--

(1) Are familiar with the contents of this AMC regulation and the references listed in appendix A.

(2) Participate in the review of all plans, in staff organizations and meetings addressing force protection issues, and in force protection exercises.

(3) Provide advice to operational crisis action teams and task forces.

(4) Maintain timely, complete technical channel communications with their counterparts at subordinate, lateral, and higher headquarters.

c. *Jurisdiction*. Legal officers will be particularly alert to the issues enumerated below. These issues are recurring and complex, and their solutions are situation-dependent.

(1) General - United States. Federal, State, and local officials have overlapping responsibilities for the detection, investigation, and prosecution of criminal offenses.

(2) United States Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI). The Attorney General (AG) is the head of DOJ and, acting through DOJ’s officials, bears the primary responsibility for enforcement of Federal laws. As part of DOJ, the FBI detects and investigates crimes against the United States. The FBI has overall responsibility at the scene of a domestic terrorist incident wherever it occurs, including military installations. Under the direction of the AG, the conduct of litigation in which the United States is a party, or in which it is interested, and the securing of evidence therefore, is reserved to officers of DOJ.

(3) DOD, Department of the Army (DA), AMC, and AMC Installation and Units. DOD/DA/AMC/AMC Installation and units are responsible for the security of their facilities, property, and personnel. This includes the responsibility for investigating crimes committed on military installations and crimes committed by persons subject to the Uniform Code of Military Justice. DOD/DA/AMC/AMC installations and units coordinate investigative and prosecutorial activities with DOJ and the FBI per established guidelines.

(4) State and Local Law Enforcement and Prosecutorial Agencies. At the State and local level, these agencies perform functions similar to those of DOJ/FBI. To coordinate investigative and prosecutorial activities at the state and local level, AMC installations and units establish local policies and procedures with competent state and local authorities.

(5) General - OCONUS. The Host Nation may have responsibility for detection, investigation, and prosecution of criminal offenses occurring at AMC activities located outside of the United States. Such affected AMC activities should, through the designated United States Defense Representative for the country and Chief of Mission, establish local arrangements with Host Nation authorities for these matters. These AMC activities will ensure their actions are coordinated with the Office of the Staff Judge Advocate (OSJA) for the senior U.S. Army Command responsible for the geographical area, e.g., OSJA, U.S. Army Europe (USAREUR) for Germany and OSJA, Southern European Task Force (SETAF) for Italy.

d. *Rules for the Use of Force (RUF) and Rules of Engagement (ROE)*. In any operational situation, competent authority will issue RUF/ROE tailored to the mission. Under all circumstances, every soldier retains the inherent right of self-defense.

e. *Posse Comitatus Act*. The Posse Comitatus Act prohibits the use of Army personnel to execute the civil laws of the United States, "except in cases and under circumstances expressly authorized by the Constitution or Act of Congress." This prohibition is against direct military involvement in civilian law enforcement. Generally, military support short of actual search, seizure, arrest, or similar confrontation with civilians, e.g., traffic direction is not a violation of the Act. The Act does not prohibit actions taken for the primary purpose of protecting military facilities, property, and personnel.

f. *Intelligence gathering*. Certain DOD/DA intelligence and law enforcement agencies are authorized to collect, retain, and disseminate information for the protection of Defense facilities, property, and personnel. AMC Intelligence and Security personnel are not authorized to collect, retain, or disseminate such information per AR 381-10. Given Constitutional guarantees of free speech, free association, and privacy, DOD/DA intelligence

and law enforcement agencies must scrupulously adhere to the applicable policies and procedures. Generally speaking, with regard to collection, these require a legitimate category of information, the least intrusive means, and the appropriate approval authority, and with regard to retention and dissemination, these require a legitimate purpose.

g. *Command and signal*.

(1) For unsecure voice communications with AMC COMMAND COUNSEL, use (703) 617-8031/8032/0238. (NOTE: The DSN prefix is 767.)

(2) For secure voice (STU III) communications with AMC COMMAND COUNSEL, use (703) 617-8031/8032/8048. (NOTE: The DSN prefix is 767.)

(3) For unsecure facsimile communications with the AMC COMMAND COUNSEL, use (703) 617-5680. (NOTE: The DSN prefix is 767.)

5-26. Chemical/biological. a. FP Plans will describe procedures for protecting soldiers, civilian employees, family members, facilities and equipment at AMC installations against chemical and biological (CB) agent attacks. Commanders will ensure all AMC personnel and installations are provided information and guidance for protecting the force during CB situations.

b. AMC chemical activities/depots are specifically guided by AR 50-6, 385-61 and AR 190-59 for safety and security requirements.

c. The CB threat must be continually analyzed. Installation commanders must consider potential CB threats in local threat assessments and contingency/disaster plans. Installation Commanders will--

(1) Analyze the CB threat as part of the overall Physical Security Plan (PSP) during local threat assessments.

(2) Develop CB response procedures for disaster/ contingency plans.

(3) Contact the U.S. Army Soldier and Biological Chemical Command (SBCCOM) Operations Center if technical assistance or specialized teams are required. Chemical capabilities include: render safe operations, detection/identification, physical protection, and decontamination. SBCCOM will coordinate biological agent technical assistance with the U.S. Army Medical Research Institute for Infectious Disease (USAMRIID).

(4) Report all CB incidents through their normal chain of command and to the AMC EOC.

(5) Ensure the Special Reaction Team (SRT) is adequately equipped and trained in order to react to the CB threat and/or incident.

(6) Memorandums of Agreement (MOA) and/or local emergency response plans/mutual aid agreements will be coordinated with local fire, police, and health authorities, as appropriate.

d. *Communications*. Telephone numbers and other electronic addresses are as follows:

(1) SBCCOM Operation Center.

Voice phone:
Duty Hrs - DSN 584-2933
COMM 410-671-2933
Nonduty - DSN 584-2148
COMM 410-671-2148
FAX phone: DSN 584-4496
COMM 410-671-4496
E-mail: AMSCBOC@apgea.army.mil

(2) AMC EOC:

Voice phone: DSN 767-8406
COMM 703-617-8406
FAX phone: DSN 767-2935
COMM 703-617-2935
E-mail: AMCOC@HQAMC.army.mil

5-27. Medical response and consequence management.

a. *General*. Medical response planning at all levels of command within AMC is an essential FP function. If an incident occurs, timely medical response is critical to provide appropriate levels of trauma treatment, minimize loss of life, and protect against additional injury subsequent to the event. Prior coordination of response details, proper consequence management, and exercise of the response plan are essential in ensuring optimal care is delivered at the incident scene, in medical treatment facilities, and in the organization after the event.

b. *Concept*. Installation operations personnel will develop a plan of action to provide on-site medical response. Details will be closely coordinated with the Installation Medical Authority (IMA) and local and regional emergency preparedness officials, as required, based on installation specific circumstances.

c. *Execution*. Consider the following in developing the response plan:

(1) Threat analysis. The IMA must analyze the various proposed scenarios, assess the capabilities available, and determine any additional requirements for training, personnel, or equipment.

(2) Availability of responders. Subordinate AMC units are located at a wide variety of types of installations with different levels of medical support. In many situations, only emergency medical treatment (EMT) support is available on the installation. There are three general types of medical support scenarios.

(a) Medical personnel available, chemical weapons on site. These installations already have a detailed chemical accident response plan. Installation operations personnel should tailor the responses specified in that plan to nonchemical emergencies to meet the FP requirement.

(b) Medical personnel available, no chemical weapons on site. The clinic already has a mass casualty plan. Some adjustments will be required to include terrorist attack scenarios.

(c) No medical personnel available. In the absence of medical personnel on site, agreements with local jurisdictions are in place to provide emergency medical response. Such agreements must be revised to include terrorist attack scenarios.

(3) Site specific considerations. The IMA and the AMC installation or tenant unit commander must carefully coordinate to ensure the potential for exposure of responders to hazardous chemicals, nuclear and/or biological contaminates, the risk of explosion, or other site-specific industrial hazards is recognized in developing the response plan and consequent management.

(4) Communications. Medical response resources must be able to communicate with the emergency operations center. Communications exercises must be conducted to verify voice and data communications systems are functional.

(5) Psychological effects. Military mental health services are not commonly found at AMC installations. Emergency response plans typically do not provide for posttraumatic psychological counseling necessary following a terrorist attack. The need for trained mental health professionals to provide counseling must be included in coordinating with the supporting military and civilian medical treatment facilities.

(6) External support. Regardless of the availability of first responders on the installation, coordination must be made to provide hospital based out-patient and in-patient care for casualties. Installation personnel must review support and mutual aid agreements to ensure sufficient treatment capacity can be

accessed to accommodate casualties from a terrorist attack. Availability of medical evacuation assets must be included in the review.

d. *Coordination*. Operational control of supporting Army medical assets is located at the Regional Medical Command (RMC). Medical response plans and requests for services should be coordinated through the local treatment facility, the supporting Medical Department Activity (MEDDAC) and the RMC.

e. *Exercises*. Response plans developed for force protection must be exercised regularly to be effective. Such exercises may be held in conjunction with other requirements. Hospitals and clinics must conduct mass casualty exercises. There are requirements for exercising medical response to chemical accidents. Holding FP response exercises in conjunction with other existing exercise requirements will benefit the FP effort without overburdening the agencies involved. It is critical that agencies external to the installation actively participate in all exercises.

5-28. Safety. a. Safety planning and execution at all levels of command within AMC is essential to FP programs. During planning and execution, commanders and staffs will use risk management procedures to identify and control mission hazards. The risk management model includes five steps: 1) identify hazards, 2) assess hazards, 3) develop controls and make risk decisions, 4) implement controls, and 5) evaluate. For each threat situation, risk management procedures should be used to identify the hazards that result in the greatest risk to the mission, including personnel and public safety.

b. Installation staffs will coordinate with appropriate local emergency response authorities to review mutual aid agreements and/or notification for contingency/disaster preparedness and threat scenarios. Installation safety personnel will continuously integrate safety requirements and identify hazards in preparation for worst case scenarios. Activities that contribute to preparing for the threat include (but are not limited to): planning, review of SOPs, training, exercises and evaluation.

c. Commanders will ensure that all AMC personnel and installations are provided information and guidance for protecting the force during situations where personal safety is threatened.

d. Staffs will advise the Commander of below-standards status that could affect force protection. Safety concerns related to FP will be addressed to the FP Working Group for resolution.

5-29. Force protection training. a. *General*. Force Protection training requirements and standards for organizations, installations, and individuals will be implemented at all AMC command levels. Force Protection training initiatives exist to ensure that Force Protection knowledge and awareness are

emphasized at all levels. Individual security awareness and protection training are essential elements of the overall force protection program. Each individual must share in this responsibility by ensuring the proper degree of alertness and support of personal protection measures. The objectives of the Force Protection training initiatives are the following:

(1) Instill an active Antiterrorism/Force Protection mindset in all personnel.

(2) Train commanders and staff to integrate Force Protection and risk management considerations into all operations and activities.

(3) Direct specialized training for key personnel performing force protection duties.

(4) Increase the knowledge and awareness of all individuals in the recognition of possible threats and vulnerabilities, hazards, and recommended countermeasures.

(5) Arrange for region specific training for deploying individuals and organizations.

(6) Include Force Protection into organization training exercises.

b. *Training Program Levels*. The U.S. Army Force Protection training guidance consists of four levels of Antiterrorism/Force Protection training. This section implements the MACOM portion of the Levels I and II instructions of the Army program at AMC. Levels III and IV training are managed at HQDA. The following is a list of the four levels of training described in the U.S. Army program:

(1) Level I: Individual Awareness Training.

(2) Level II: Key Force Protection Personnel Training.

(3) Level III: LTC/COL Pre-command Course Training.

(4) Level IV: Executive Level Seminar (COL - MG level).

c. *Level I Training*. Level I training provides individual antiterrorism awareness training to soldiers, DA civilians, contractors, and family members deploying or traveling outside the 50 United States, its territories, and possessions. Level I training must be accomplished within 6 months prior to deployment/travel. Level I consists of two categories: (1) training required for deployment to negligible/low threat areas; and (2) training required for medium or higher threat areas.

(1) Level I minimum training standards for deployments to negligible/low threat areas are items listed below. Level I (negligible/low threat) training does not require a Level II qualified instructor.

(a) View the current Army's Force Protection/ Antiterrorism training videos, Introduction to Terrorism, Terrorism Operations, and Individual Protective Measures.

(b) Receive and read JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to combating Terrorism" July 1996 and OCJCS pocket card (PC) 5260, or GTA 19-4-3, a pocket booklet entitled "Individual Protective Measures for Personal Security" July 1997.

(c) Receive a current update on the area of travel.

(2) Level I minimum training standards for deployment to medium or higher threat areas are the following:

(a) The same requirements as Level I (negligible/low threat areas), plus the additional videos: Detecting Terrorist Surveillance and Hostage Survival.

(b) Instruction by a qualified instructor using the lesson plans, which have been prepared or approved by the U.S. Army Military Police School. A qualified instructor is an individual who has completed Level II training; or, an individual who has received formal training in antiterrorism individual protection. A Colonel (O-6) is the lowest level authorized to designate qualified instructors of those who have not completed level II training.

(3) The Level I Program of Instruction is available for issue from the U.S. Army Military Police School by letter request signed by O-6 Commander to--

Commandant
U.S. Army Military Police School
ATTN: ATZN-MP-TD
Ft McClellan, AL 36205-5030

(4) The Level I Program of Instruction consists of the following subjects:

(a) Introduction to Terrorism (RJ1200).

(b) Terrorism Operations (RJ1205).

(c) Individual and Unit Protective Measures (RJ1215).

(d) Hostage Survival Techniques (RJ1225), Medium or High threat areas.

(e) Terrorist Surveillance Detection (RJ1235), Medium or High threat areas.

d. *Level II Training*. Level II training has the following objectives:

(1) Prepare individuals to manage force protection programs and provide subject matter expertise to the organization commander.

(2) Train and certify individuals who can provide Level I training at the organization and installation level.

(3) The target audience for Level II Training includes E-6 through O-4, warrant officers, and civilians.

(4) The formal training course entitled, "The Force Protection Unit Advisors Course," at the U.S. Army Military Police School and the "Antiterrorism Instructor Qualification Course," at the John F. Kennedy Special Warfare Center and School, satisfies the Level II Training requirements.

e. *Tasks and responsibilities*.

(1) MSC/SRA commanders/directors:

(a) Provide for the training of key installation and organization Force Protection personnel at their appropriate levels. Commanders will ensure that key personnel are identified/released and that funds are programmed for formal staff training. It is mandatory that Force Protection managers and specialists in the types of positions listed below attend formal qualifying training courses:

1 Force Protection Officers and their assistants.

2 Physical Security Specialists.

3 Intelligence Personnel.

4 Information Assurance (information systems security) staff.

5 Persons presenting Force Protection Briefing and Training.

(b) Ensure training exercises (CPX, FTX, etc.), include integrated scenarios of terrorist threats, THREATCON procedures, attacks and consequence management.

(c) Ensure high-risk personnel and individuals assigned to high-risk positions attend the Individual Terrorism Awareness Course (2A-F40/011-F21, (5 days) U.S. Army JFK Special Warfare Center, Fort Bragg, NC), or equivalent, prior to

initiation of overseas travel.

(d) Ensure DOD personnel deploying OCONUS receive focused Level I training on Antiterrorism/Force Protection prior to deployment. These personnel include individual soldiers, DOD civilians, and their family members whether deploying as part of a unit, as an individual staff augmentee or unit filler, on TDY, permanent change of station (PCS) or leave. Provide DOD contractors training when they are traveling OCONUS as part of contractual operations. Training will include the following topics:

1 Self-protection measures.

2 Potential threats in the areas of travel.

3 Avoiding/overcoming routine behavior patterns.

4 Maintaining a low profile.

5 Being sensitive to change in the security atmosphere.

6 Being prepared for unexpected events.

7 Working environment awareness.

8 Visitor control.

9 Social and recreational activities awareness.

10 Air, rail, and sea travel awareness.

11 Information specific to the travel areas on how to respond to suspicious incidents.

12 All other training requirements as determined by the gaining commander-in-chief (CINC) and within the MSC's/ SRA’s ability to provide.

(e) Ensure that leaders of units deploying OCONUS receive additional training focusing on their Force Protection leadership responsibilities, including risk management.

(f) Ensure training is provided to enhance travel security of individuals while en route on OCONUS PCS. (The gaining command will be responsible for providing more detailed training when the soldier or DOD civilian arrives.) Provide soldiers and DOD civilians scheduled for an OCONUS PCS a tailored threat awareness briefing. The briefing will focus on the soldier's mode of travel and hotel security tips relevant to the

gaining command. Family members traveling with a soldier or DOD civilian for an OCONUS PCS will be offered the opportunity to attend the threat awareness briefing.

(g) Document that individuals have received training prior to OCONUS travel. Documentation includes the individual's standard name line and the date and of the training by notations in individual training, personnel records, or a memorandum certifying that the individual has received the training. Establish procedures that verify the training for the office issuing orders and that serve as the authority to release orders to the traveler.

(h) Identify key positions in their commands that require formal or refresher Force Protection training (including risk management) prior to assumption of duties. These recommendations will be passed to HQ AMC (AMCPE) for consolidation to HQDA DCSPER to ensure that assignment orders clearly delineate special instructions for training prior to assignment.

(i) Document the family members' choice to accept or decline the travel security briefing on installation clearance papers for soldiers on PCS orders to an OCONUS assignment.

(j) To the maximum extent possible, provide Level I training support for members of other AMC elements and individuals geographically separated from their parent organizations.

(2) HQ AMC responsibilities.

(a) AMCLG-OF.

1 Serve as the overall point of contact for the AMC Force Protection Training Program.

2 Develop and implement the AMC Force Protection Training Program.

3 Obtain and allocate quotas for the Force Protection Unit Advisor’s Course (Level II training/ certification) and the Level IV executive level training seminar.

4 Distribute ISS/IA policy and in coordination with AMCIO, implementation procedures.

5 Coordinate through channels with the theater CINC or gaining OCONUS commander to obtain Force Protection training requirements and information specific to the target area of operations.

6 Serve as the point of contact for AMC Level I training and travel security information.

7 Implement the Level I training program for AMC.

8 Develop and distribute travel security guidelines and briefing materials.

(b) AMCMI.

1 Prepare and/or schedule SAEDA briefings, which include terrorist threat section, for all personnel on a biennial basis.

2 Contribute to the development of travel threat and security guidelines for use by the AMC FP Office in preparing Level I Travel briefings.

3 Contribute to the development of force protection scenarios for training exercises.

(c) AMCPE.

1 Identify for travel security briefings and training the HQ, AMC military and DA civilian personnel traveling/deploying/PCSing OCONUS and include mandatory FP Level I Training requirements on all overseas travel/deployment orders. Provide the names/destinations of OCONUS travelers to AMCLG-OF.

2 Retain TDY, PCS or leave orders of OCOUNS-bound personnel until they are certified by AMCLG-OF as Level I trained for their destinations.

(d) AMCPE-S.

1 Serve as subject matter expert for development of physical security and high-risk personnel training and briefing materials.

2 Serve as AMC point of contact for Special Reaction Team training.

3 Serve as AMC point of contact for evasive driver training.

4 Contribute to development of force protection scenarios for training exercises.

(e) AMCCH.

1 Serve as the subject matter expert for information regarding beliefs and practices of distinctive faith groups and factions. Assist AMCLG-OF, AMCMI, AMCPE, and AMCPE-S in preparation of materials for training, travel, and security briefings as appropriate for military purposes.

2 Assist commanders at all levels in understanding of specific requirements and practices so that effective decisions can be made in those instances where religious beliefs and practices are claimed to be in conflict with military directives.

5-30. Reports. a. *Terrorist Threat Report (TTR).* Per AR 525-13, a Terrorist Threat Report (using OPREP-3 format) is required when credible information is received about a planned attack against U.S. Army personnel, facilities or assets. Information is considered credible if it warrants a change in the THREATCON or an increase to current security measures. Additional reporting procedures and requirements are contained in AR 525-13 (Appendix D), and Chairman of the Joint Chiefs of Staff Instruction, CJCSI 3150.03, dated 1 DEC 93.

(1) TTR time requirements.

(a) If there is credible information of a possible attack or incident, provide the information immediately by telephone to the Army Operations Center and as soon as possible thereafter to the AMC Operations Center.

(b) A follow-up OPREP-3 will be transmitted within 6 hours of receiving the original threat information to the Army Operations Center and to AMC HQ (AMCLG-OF).

(c) Updates to TTR messages are required as soon as new information becomes available or at least once every 12 hours.

(2) TTR Addressees. TTR messages should be addressed to the following: HQDA (MSG address: DA WASH DC//DAMO-AOC/DAMO-ODL-FP/DAMO-ODO/DAMI-CHI//), CID Command (CDRUSACIDC WASH DC//CIOP-IN//), INSCOM (CDRINSCOM FT BELVOIR VA//IAOPS-IS//); HQ AMC (CDRAMC ALEXANDRIA VA//AMCLG-OF//), and the regional commander (e.g., FORSCOM (COMFORSCOM FT MCPHERSON GA//AFOP-OCO/AFPM-FP/AFIN-IS//).

b. *Terrorist Incident Report (TIR).* Per AR 525-13, a TIR (using OPREP-3 format) will be submitted when a terrorist incident or suspected terrorist incident occurs against U.S. Army personnel, facilities, or assets.

(1) TIR time requirements.

(a) Initial TIRs will be provided immediately by telephone to the Army Operations Center and as soon as possible thereafter to the AMC Operations Center.

(b) Telephonic updates will be every even hour for the duration of an incident to the Army Operations Center (AOC) and the AMC Operations Center.

(c) An electronic message with all available details of the incident, security measures in effect, and actions taken since the attack will be submitted within 6 hours of the incident to the AOC and AMC Operations Center.

(2) TIR submission requirements and addressees.

(a) Initial TIRs will be provided telephonically to the Army Operations Center (AOC DSN: 227-0218/9; Comm: (703) 697-0218/9 and the HQ AMC Operations Center (DSN: 767-8406/8407; Comm (703) 617-8406/8407).

(b) TIR Addressees. TIR messages should be addressed to the following: HQDA (MSG address: DA WASH DC//DAMO-AOC/DAMO-ODL-FP/DAMO-ODO/DAMI-CHI//), CID Command (CDRUSACIDC WASH DC//CIOP-IN//), INSCOM (CDRINSCOM FT BELVOIR VA//IAOPS-IS//); HQ AMC (CDRAMC ALEXANDRIA VA//AMCLG-OF//), and the regional commander (e.g., FORSCOM (COMFORSCOM FT MCPHERSON GA//AFOP-OCO/AFPM-FP/AFIN-IS//).

c. *After action report*. Per AR 525-13, a comprehensive after action report of the terrorist threat or incident is required within 30 days. MSC commanders and SRA directors are required to forward a complete report of the threat or incident, including lessons learned to HQ AMC (AMCLG-OF). HQ AMC will compile and forward the final after action report to HQDA (DAMO-ODL-FP) and to the Center for Army Lessons Learned (CALL).

d. *THREATCON reports*. THREATCON reports will be submitted per AR 525-13 and this regulation. The following instructions are in addition to the instructions contained in AR 525-13.

(1) Commanders/directors of MSCs/SRAs will report changes to THREATCONs to HQ AMC Operations Center (AMCLG-OF) within 2 hours by telephone DSN 767-8406/7. The telephonic report will be followed up within 6 hours by a facsimile or electronic message to HQ AMC Operations Center (AMCLG-OF), facsimile DSN 767-2935 or secure facsimile DSN 767-7312.

(2) HQ AMC Operations Center (AMCLG-R0) will monitor the status of THREATCONs for subordinate commands and report subordinate and commandwide THREATCON changes to HQDA. The monthly MACOM THREATCON status will also be reported by AMC HQ (AMCL-RO) to HQDA.

(3) HQ AMC Operations Center (AMCLG-R0) will submit monthly THREATCON to HQDA per AR 525-13.

e. The following reports are required by this regulation:

(1) Command Force Protection Assessment: MSC/SRA commanders submit annually by 15 November.

(2) Terrorist Threat Report: All organization elements submit a TTR (using the OPREP-3 format) when there is a credible terrorist threat.

(3) Terrorist Incident Report: All organization elements submit a TIR (using the OPREP-3 format) when a terrorist incident or suspected terrorist incident occurs.

(4) THREATCON status: MSC/SRA commanders will submit THREATCON status monthly to HQ AMC Operations Center (AMCLG-R0). THREATCON changes will be reported to HQ AMC Operations Center (AMCLG-R0) within 2 hours of the change.

The proponent of this regulation is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, HQ AMC, ATTN: AMCLG-OF, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

NORMAN E. WILLIAMS
Major General, USA
Chief of Staff

LEROY TILLERY
Chief, Printing and Publications
Branch

DISTRIBUTION:
Initial Distr H (44) 1 ea HQ Acty/Staff Ofc
LEAD (SIOLE-DO-I) (2)
AMCIO-I-SP stockroom (15)
Separate Reporting Activities (SRA) (2 ea)
AMCOM/AMSAM-RM-FD (4)
AMCOM/AMSAM-SMO (Library) (4)
ARL/AMSRL-CI-TG (4)
CECOM/AMSEL-IM-BM-I (4)
IOC/AMSIO-IMC (4)
LOGSA/AMXLS-IM (4)
SBCCOM/AMSCB-CIH (4)
STRICOM/AMSTI-CS (4)
TACOM/AMSTA-RM-DCR (4)
TECOM/AMSTE-CT-N (4)
USASAC/AMSAC-IM-O (4)

APPENDIX A

REFERENCES

SECTION I. Required References

AR 190-13
The Army Physical Security Program, September 1993.

AR 190-27
Army Participation in the National Crime Information Center

AR 190-45
Law Enforcement Reporting

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 190-58
Personal Security

AR 195-2
Criminal Investigation Activities

AR 360-5
Army Public Affairs, Public Information, and the AMC Supplement.

AR 380-13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 380-19
Information Systems Security, and the AMC Supplement.

AR 380-53
Information systems Security Monitoring

AR 381-10
U.S. Army Intelligence Activities

AR 381-12
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 415-15
Army Military Construction Program Development and Execution

AR 525-13
The Army Combating Terrorism Program -- Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources

AR 525-20
Command and Control Countermeasures (C2CM)

AR 530-1 and AMC Supplement to AR 530-1
Operations Security (OPSEC)

DA PAM 190-51
Risk Analysis for Army Property

DODD 2000.12
DOD Combating Terrorism Program

DOD Handbook 2000.12H
Protection of DOD Personnel Against Terrorists Acts

DODI 2000.14
DOD Combating Terrorism Program Procedures

DODI O-2000.16
DOD Combating Terrorism Program Standards

FM 100-14
Risk Management

GTA 21-3-11
Individual Protective Measures (or locally produced equivalent)

Joint Pub 3-07.2
Tactics, Techniques, and Procedures for Antiterrorism

JS Guide 5260
Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism

TM 5-853-1
Security Engineering, Project Development

TM 5-853-2
Security Engineering, Concept Design

TM 5-853-3
Security Engineering, Final Design

TM 5-852-4
Security Engineering, Electronic Security Systems

SECTION II. Related References

C2 Protect & Intelligence

AR 380-5 and AMC Supplement to AR 380-5
Department of the Army Information Security Program

AR 380-10
Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives, 30 December 1994.

AR 380-28
Department of the Army Special Security System - Sensitive Compartmented Information

AR 380-40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 380-67
Personnel Security Program, 9 Sep 88, and the AMC Supplement.

AR 381-20
The Army Counterintelligence Program

AR 381-100
Army Human Intelligence Collection Programs(S)

ARL's Assessment of Unclassified-Sensitive AIS, 10 Mar 97.

DODD 5240.1
DOD Intelligence Activities, 25 April 1988.

DOD 5240.1-R
Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, December 1982.

FM 34-60
Counterintelligence

Message, DA (DAMO-ODI), DTG 201912A SEP 96, subj: Activation of the ACERT/Coordination Center (CC).

Chaplain Services

FM 16-1
Religious Support

Law Enforcement, Physical Security, and Personal Security

AR 55-46
Travel Overseas

AR 190-11
Physical Security of Arms, Ammunition and Explosives

AR 190-14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties, 12 March 1993.

AR 190-16
Physical Security

AR 190-30
Military Police Investigations

AR 190-56
The Army Civilian Police and Security Guard Program

AR 500-50
Civil Disturbances

AR 500-51
Emergency Employment of Army and Other Resources - Support to Civilian Law Enforcement

DODD 5525.5
DOD Cooperation with Civilian Law Enforcement Officials, 15 January 1986.

DODI 5210.84
Security of DOD Personnel at U.S. Missions Abroad, 22 January 1992.

FM 19-10
The Military Police Law and Order Operations

FM 19-15
Civil Disturbances, 25 November 1985.

FM 19-20
Law Enforcement Investigations

FM 19-30
Physical Security

Legal
AR 27-10
Military Justice, 24 June 1996.

18 U.S.C. § 1385 (Posse Comitatus Act).

Agreement Governing the Conduct of the Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigations, 5 April 1979 (reprinted in AR 381-10).

Memorandum of Understanding Between the Department of Defense, the Department of Justice, and the FBI on Use of Military Force in Domestic Terrorist Incidents, 5 August 1983.

Memorandum of Understanding Between the Department of Justice and Defense Relating to Investigation and Prosecution of Certain Crimes, August 1984 (reprinted in AR 27-10).

Medical Response and Consequence Management

AR 50-6
Chemical Surety

DA PAM 50-6
Chemical Accident or Incident Response and Assistance (CAIRA) Operations

FM 3-4
NBC Protection

FM 3-5
NBC Decontamination

FM 3-21
Chemical Accident Contamination Control

FM 3-100
Chemical Operations, Principals, and Fundamentals

FM 8-9
NATO Handbook on the Medical Aspects of NBC Defensive Operations

FM 8-10-7
Health Service Support in a Nuclear, Biological and Chemical Environment

FM 8-55
Planning for Health Service Support

FM 8-285
Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries

MEDCOM Reg 525-4
Military Operations Emergency Preparedness

Plans and Operations

AR 530-1
Operations Security (OPSEC)

DOD Civilian Disturbance Plan (GARDEN PLOT), 15 February 1991.

DODD 3025.1
Military Support to Civil Authorities, 15 January 1993

DODD 3025.12

Military Assistance for Civil Disturbances, 4 February 1994.

FM 100-5
Operations

FM 100-19
Domestic Support Operations

FM 100-37
Terrorism Counteraction, July 1987.

FM 101-5
Staff Organization and Operation

Public Affairs
AR 360-61
Community Relations

AR 360-81
Command Information Program

SAFETY
AR 385-10, The Army Safety program

AR 385-40, Accident Reporting and Records

AR 385-61, The Army Chemical Agent Safety Program

AR 385-64, Army Explosives Safety Program

AR 385-69, Biological Defense Safety Program

AR 385-80, Nuclear Reactor Health and Safety

GLOSSARY

SECTION I. Abbreviations

ACERT	Army Computer Emergency Response Team
AG	Attorney General
AIG	Automated Information Group
AIS	Automated Information System
AMC	Army Materiel Command
AMG	Alarm Monitor Group
AOC	Army Operation Center
AR	Army Regulation
AT	Antiterrorism
AWOL	Absent Without Leave
BASOPS	Base Operating (Information) System
CALL	Center for Army Lessons Learned
CB	Chemical and Biological
CBT	Computer Based Training
CCTV	Closed Circuit Television
CDR	Commander
CG	Commanding General
CID	Criminal Investigation (Command) Division
CIDS	Commercial Intrusion Detection System
CINC	Commander-in-Chief
COMSEC	Communications Security
CONUS	Continental United States
COOP/DRP	Continuity of Operations/Disaster Recovery Plan
CPAC	Civilian Personnel Advisory Center

CPM	Command Provost Marshal
CPOC	Civilian Personnel Operations Center
CT	Combating Terrorism
DA	Department of the Army
DCS	Deputy Chief of Staff
DCSINT	Deputy Chief of Staff for Intelligence
DCSPER	Deputy Chief of Staff for Personnel
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOJ	Department of Justice
DSS	Defense Security Service
EMT	Emergency medical treatment
EOC	Emergency Operations Center
ESS	Electronic Security Systems
FBI	Federal Bureau of Investigation
FIO	Foreign Intelligence Office/Officer
FIS	Foreign Intelligence Service
FM	Field Manual
FOUO	For Official Use Only
FP	Force Protection
FPAT	Force Protection Assistance Team
FPMO	Force Protection Management Office
FPO	Force Protection Office/Officer
FPP	Force Protection Program/Plan

GO	General officer
HQ	Headquarters
HQDA	Headquarters, Department of the Army
HRP	High Risk Personnel/Position
IA	Information Assurance
I&S	Intelligence and Security
IDS	Intrusion Detection System
IMA	Installation Medical Authority
INSCOM	Intelligence and Security Command
INTSUM	Intelligence Summary
IP	Internet Protocol
ISS	Information Security System
J-SIIDS	Joint Services Interior Intrusion Detection System
LIWA	Land Information Warfare Activity
MACOM	Major Army Command
MCWG	Military Construction Working Group
MDARS	Mobile Detection Assessment Response System
MDEP	Management Decision Package
MEDDAC	Medical Department Activity
MEVA	Mission Essential Vulnerability Area
MI	Military Intelligence
MOA	Memorandum of Agreement
MPMIS	Military Police Management Information System
MSC	Major Subordinate Command
MWD	Military Working Dog
NCR	National Capital Region
OCONUS	Outside the Continental United States

OMA	Operations and Maintenance Authorization
OPR	Office of Primary Responsibility
OPREP-3	Operational Report
OPSEC	Operations Security
OSJA	Office of the Staff Judge Advocate
PA	Public Affairs
PAO	Public Affairs Office/Officer
PBAC	Process Budget Advisory Committee
PC	Pocket Card
PCS	Permanent Change of Station
PM	Provost Marshal
POM	Program Objective Memorandum
PR	Production Requirement
PSEMO	Physical Security Management Office
PSP	Physical Security Program
QLPR	Security & Law Enforcement MDEP
QRR	Quick Reaction Requirement
QSEC	Director of Security MDEP
RAC	Resource Action Committee
RACS	Registration and Access Control System
RDA	Research, Development, Acquisition
RDTE	Research, Development, Testing and Evaluation
RFI	Request For Information
RIC/RAC	Resource Integration Committee/Resource Action Committee
RJC6	MDEP for physical Security
RM	Resource Management
RMC	Regional Medical Command

ROE	Rules of Engagement
RUF	Use of force
SAEDA	Sabotage and Espionage Directed Against the Army
SAV	Staff Assistance Visit
SBCCOM	Soldier and Biological Chemical Command
SCIF	Sensitive Compartment Information Facility
SETAF	Southern European Task Force
SIGINT	Signals Intelligence
SII	Statement of Intelligence Interest
SIO	Senior Intelligence Officer
SJA	Staff Judge Advocate
SM	Security Manager/Office
SMS	Security Management System
SOP	Standard Operating Procedures
SRA	Separate Reporting Activity
SRT	Special Reaction Team
SSD	Security Support Division
TBB	Target Based Budgeting
TDY	Temporary Duty
THREATCON	Threat Condition
TIR	Terrorist Incident Report
TTR	Terrorist Threat Report
UFR	Unfunded Requirements
USAMRIID	U.S. Army Medical Research Institute for Infectious Diseases
USAREUR	U.S. Army Europe
VTER	Antiterrorism MDEP

AMC Primary Staff Indicators

AMCCC	Command Counsel
AMCCH	Command Chaplain
AMCEN	DCS for Engineering
AMCIO	DCS for Corporate Information
AMCLG	DCS for Logistics (AMCLG-OF: Force Protection Office)
AMCMI	DCS for Intelligence
AMCPA	Command Public Affairs Office
AMCPE	DCS for Personnel (AMCPE-S: Security and Law Enforcement)
AMCRM	DCS for Resource Management
AMCSF	Command Safety Office
AMCSG	Command Surgeon

SECTION II. Definitions and Terms

Information assurance/C2 Protect Related Terms

Authentication
A security measure designed to protect a communications system against acceptance of fraudulent transmissions or simulation by establishing the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Availability
The state when data is in the place needed by the user, at the time the user needs it, and in the form needed by the user.

Confidentiality
The concept of protecting data from unauthorized disclosure.

Integrity
The degree of protection for data from intentional or unintentional alteration or misuse.

Risk
The probability that a particular threat will exploit a particular vulnerability of an automated information system or telecommunications system.

Threat
Any capability, circumstance, or event with the potential to cause harm to an AIS in the form of destruction, unauthorized disclosure, modification of data, or denial of service.

Threat Agent
A means or method used to exploit a vulnerability of a system, operation, or facility.

Vulnerability
A weakness in an AIS or cryptographic system (or system procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access to classified or sensitive information, impact system availability, or affect data integrity.

FP Generalized Terms

Antiterrorism
Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts to include limited response and containment by local military forces. Also called AT.

AT Awareness
Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorist acts.

AT Resident Training
Formal classroom instruction in designated DOD courses that provide specialized instruction on specific combating terrorism topics; i.e., personal protection, terrorism analysis, regional interest, and AT planning.

Combating Terrorism
Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) taken to oppose terrorism throughout the entire threat spectrum.

Counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT.

Domestic Terrorism
Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

Family member
Individuals defined as "dependent" in Section 1072(2) OF 10 U.S.C. (reference (c)) including spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (under 21, incapable of self support or under 23 and enrolled in a full-time institution).

Force Protection
Security program developed to protect soldiers, civilian employees and family members, facilities and equipment, in all locations and situations. This is accomplished through the planned integration of combating terrorism (AT/CT), physical security, information operations, personal security and law enforcement operations, all supported by the synchronization of operations, intelligence, policy and resources.

High-Risk Personnel
Personnel, who because of their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.

High-Risk Target
U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target.

Installation
A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Installation Commander
The individual responsible for all operations performed by an installation.

International (or transnational) Terrorism
Terrorism in which planning and execution of the terrorist act transcends national boundaries. In defining international terrorism, the purpose of the act, the nationalities of the victims, or the resolution of the incident are considered. Those acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists.

Operations Security
A process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Physical Security
That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft.

Prevention
The security procedures undertaken by the public and private sector in order to discourage terrorist acts.

Special Reaction Team
A unit of specially trained military or DOD police personnel operating under the auspices of the Provost Marshal, the Chief of Security, or the Chief of Security Police, armed and equipped to respond to and to resolve special threat situations above and beyond the scope of standard or usual law enforcement capabilities.

Terrorism
The calculated use or use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorist
An individual who uses violence, terror, and intimidation to achieve a result.

Threat Analysis
In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of a terrorist group’s existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment.

Threat and Vulnerability Assessment
In antiterrorism, the pairing of a facility’s threat analysis and vulnerability analysis.

Terrorist Threat Conditions
A CJCS-approved program standardizing the military services' identification of and recommended responses to terrorist threats against U.S. personnel and facilities. Also called THREATCONs, this program facilitates interservice coordination and support for antiterrorism activities. There are four THREATCONs above normal:

a. THREATCON ALPHA: This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONs resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

b. THREATCON BRAVO: This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

c. THREATCON CHARLIE: This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

d. THREATCON DELTA: This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized condition.